

1 RESUMED AT 1:05 P.M.)

2

3 MR. KENNEDY: GOOD AFTERNOON, YOUR HONOR.
4 I'LL BE EXAMINING ON BEHALF OF CYLINK. I BELIEVE
5 MR. FLINN MAY THEN HAVE A COUPLE QUESTIONS ON BEHALF
6 OF STANFORD, AND I UNDERSTAND MR. SCHLAFLY WILL HAVE
7 SOME QUESTIONS ON HIS OWN BEHALF.

8

CROSS-EXAMINATION

9

BY MR. KENNEDY: Q. GOOD AFTERNOON,
10 MR. KONHEIM. YOU'LL NOTICE WE'VE PUT UP HERE A BLOW
11 UP OF CLAIM ONE FROM THE PATENT. AND JUST TO GET TO
12 BASICS, YOU'D AGREE WITH ME THAT THE WORD
13 CERTIFICATION NOWHERE APPEARS IN THAT CLAIM?

14 A. THAT'S QUITE CORRECT.

15 Q. NOR WILL ANY OTHER CLAIMS IF WE PUT THEM UP AS
16 WELL.

17 A. I AGREE.

18 Q. AND THAT'S TRUE FOR THE WORD WARANTEE DOES NOT
19 APPEAR IN THE CLAIM?

20 A. THAT'S TRUE. IT DOES NOT APPEAR.

21 Q. AND THE WORD GUARANTEE DOESN'T APPEAR ANYWHERE IN
22 THAT CLAIM, DOES IT?

23 A. QUITE CORRECT, MR. KENNEDY.

24 Q. AND BY THE USE OF THE WORD SECURE, THAT DOES
25 APPEAR IN THE CLAIM. YOU DID NOT INTERPRET THAT TO

1 MEAN AN UNCONDITIONAL SECURE SYSTEM; CORRECT?

2 A. YES. WHEN I READ CLAIM ONE IN ITS ENTIRETY, I CAN
3 UNDERSTAND THAT COMMUNICATING SECURELY DOES NOT REFER
4 TO AN UNCONDITIONALLY SECURE SYSTEM.

5 Q. BECAUSE I THINK YOU TOLD US THIS MORNING ONE TIME
6 PADS ARE THE ONLY RECOGNIZED UNCONDITIONALLY SECURE
7 SYSTEM.

8 A. ONE TIME PADS AND THEIR VARYINGS ARE THE ONLY
9 UNCONDITIONALLY SECURE SYSTEM.

10 Q. SO WHAT YOU INTERPRETED SECURE TO MEAN HERE WAS A
11 COMPUTATIONALLY SECURE SYSTEM; CORRECT?

12 A. THAT'S CORRECT.

13 Q. AND IT'S YOUR OPINION THAT THE REASONABLE MEANING
14 OF COMPUTATIONALLY SECURE WITHIN THE ART MEANS THAT
15 SOMETHING HAS BEEN SUBMITTED TO THE CRYPTOGRAPHIC
16 COMMUNITY FOR ANALYSIS AND TESTING; CORRECT?

17 A. THAT IS MY POSITION.

18 Q. AND THE WAY ONE WOULD GO ABOUT THAT, I ASSUME, IS
19 BY PUBLISHING THEIR ALGORITHM SOMEWHERE THAT
20 CRYPTOLOGISTS ARE LIKELY TO READ IT; CORRECT?

21 A. THAT'S CORRECT.

22 Q. AND THEN YOU WAIT FOR AT LEAST TWO YEARS TO SEE IF
23 UNDER SCRUTINY AND EXAMINATION THE SYSTEM CAN BE
24 BROKEN; CORRECT?

25 A. I WOULD NOT USE THE FIGURE TWO YEARS. YOU WOULD

1 WAIT. AND THE LONGER YOU WAIT, THE LONGER THE
2 CONCERTED EFFORT IS, THE MORE CONFIDENT YOU ARE THAT
3 THE SYSTEM HAS BEEN EXAMINED AND NO PARTICULAR BREAK
4 OF THE SYSTEM HAS BEEN FOUND.

5 Q. WHAT'S THE MINIMUM PERIOD OF TIME --

6 A. I CAN'T ANSWER THAT QUESTION IN ABSTRACT. I CAN'T
7 SAY WHETHER IT SHOULD BE TWO YEARS OR FOUR YEARS. I
8 CAN ONLY JUDGE BY EXAMPLE THAT THE DATE ENCRYPTION
9 STANDARD WAS STUDIED FOR SOME FOUR YEARS BY THE
10 NATIONAL SECURITY AGENCY AND NO FAULT WAS FOUND WITH
11 IT. AND THEN IT WAS CERTIFIED BY THE NATIONAL BUREAU
12 OF STANDARDS, AND NOW IT'S GOING YEARS HENCE NO
13 ANALYSIS HAS BEEN FOUND OF D.E.S.

14 Q. SO IT COULD BE AS LITTLE AS TWO, MAYBE FOUR, MAYBE
15 MORE THAN THAT?

16 A. WELL, I WOULDN'T WANT TO AGREE ON TWO YEARS. I
17 DON'T WANT TO BE FORCED TO BE PINNED DOWN. IF I WERE
18 TO HAVE TO CHOOSE A NUMBER OF YEARS, I WOULD CHOOSE
19 THE NUMBER OF YEARS CONSISTENT WITH MY UNDERSTANDING
20 OF WHAT WAS DONE WITH D.E.S., AND SO I WOULD SAY
21 D.E.S. WAS SUBMITTED SOMETIME IN 1970, AND IT WAS
22 STUDIED.

23 AND IN '76, A CERTIFICATION WAS GIVEN. SO I
24 WOULD SAY A PRUDENT PERSON WOULD STUDY IT FOR BETWEEN
25 ZERO AND SIX YEARS.

1 Q. BEFORE BEING COMFORTABLE ABOUT MAKING THE CLAIM
2 THAT SOMETHING WAS COMPUTATIONALLY SECURE IN PATENT
3 APPLICATION; RIGHT?

4 A. BEFORE AGREEING THAT THE PHRASE COMMUNICATING
5 SECURELY IN THE SENSE OF COMPUTATIONALLY SECURE WAS
6 BEING GUARANTEED BY THE SYSTEM.

7 Q. NOW, I WANT YOU TO ASSUME THAT UNDER AMERICAN
8 PATENT LAW, IF SOMETHING HAS BEEN PUBLISHED MORE THAN
9 ONE YEAR BEFORE SOMEBODY APPLIES FOR THE PATENT,
10 THERE'S A BAR, AND YOU CAN'T GET A PATENT FOR THAT.

11 CAN YOU TELL THE COURT HOW SOMEBODY COULD
12 BOTH COMPLY WITH YOUR TIME PERIOD FOR MAKING SURE THAT
13 SOMETHING'S BEEN PROPERLY VENTED IN THE CRYPTOANALYTIC
14 COMMUNITY AND STILL HAVE SOMETHING THAT'S PATENTABLE
15 AT THE END OF PROCESS?

16 A. WELL, I COULD IMAGINE THE FOLLOWING, THAT AN
17 ARTICLE DESCRIBING THE SYSTEM IS PUBLISHED, WITHIN 12
18 MONTHS A PATENT IS FILED, BUT NOBODY OFFERS TO USE THE
19 SYSTEM UNTIL THE SYSTEM HAS BEEN CERTIFIED.

20 SO ALTHOUGH A PATENT HAS BEEN GIVEN AND MAYBE
21 ISSUED BY THE PATENT OFFICE, THE SYSTEM IS NOT USED BY
22 ANYONE UNTIL PEOPLE FEEL CONFIDENT THAT THE SYSTEM IS
23 OFFERING WHAT IT WARANTEES TO OFFER.

24 Q. NOW, CAN YOU POINT US TO A TREATISE, AN ARTICLE, A
25 GOVERNMENT PRONOUNCEMENT, MINUTES OF A

1 CRYPTOANALYTICAL SOCIETY, ANYTHING IN WRITING THAT
2 SAYS THAT'S WHAT YOU SHOULD DO BEFORE YOU CAN CLAIM
3 THAT A SYSTEM IS COMPUTATIONALLY SECURE?

4 A. WELL, I THOUGHT, MR. KENNEDY, THAT I DID THAT
5 EARLIER TODAY. EACH OF THESE ARTICLES OVER HERE
6 SUGGEST THAT IN ORDER FOR THE SYSTEM TO BE CONSIDERED
7 COMPUTATIONALLY SECURE OR COMPUTATIONALLY INFEASIBLE
8 TO GET THE KEY, THAT THE SYSTEM HAD TO -- THERE HAD TO
9 HAVE BEEN REPEATED FAILURES OF CONCERTED ATTEMPTS TO
10 BREAK THE SYSTEM.

11 FOR EXAMPLE, ON THE ARTICLE OF TRAP DOORS AND
12 KNAPSACKS AS READ ON PAGE 529. "FAITH IN THE SECURITY
13 OF THESE SYSTEMS MUST THEREFORE REST ON INTUITION AND
14 THE FAILURE OF CONCERTED ATTEMPTS TO BREAK THEM."

15 SO IT SAYS THE FAITH IN USING THE SYSTEM
16 WHETHER YOU WILL USE THIS IN THE SAME WAY YOU WOULD
17 NOT USE A DRUG WHICH HAD NOT BEEN SUITABLY TESTED
18 BEFORE WOULD DEPEND UPON ANALAYSIS -- THE DRUG
19 ANALYSIS OF THE SYSTEM BEFORE YOU WOULD ATTEMPT TO USE
20 IT.

21 Q. ASIDE FROM THOSE TWO ARTICLES FROM THE INVENTORS,
22 CAN YOU POINT US TO ANYTHING ELSE IN WRITING THAT
23 DISCUSSES BOTH THE SPECIFIC PROCESS OF APPLYING FOR A
24 PATENT AND WHAT SHOULD BE DONE TO MAKE SURE SOMETHING
25 IS COMPUTATIONALLY SECURE BEFOREHAND?

1 A. WELL, I HAVE NOT GOT MY WHOLE FILE OF PAPERS ON
2 CRYPTOGRAPHY. I'M CERTAIN THAT I COULD FIND ONE FOR
3 YOU. I'M NOT PREPARED TO GIVE AN ANSWER NOW OF PAPERS
4 THAT WOULD DEAL WITH THIS THING. BUT I'M VERY
5 CONFIDENT THAT THAT IS THE GENERALLY ACCEPTED WAY, AND
6 I KNOW THAT CERTAINLY THAT'S THE WAY THINGS WORK IN
7 THE GOVERNMENT.

8 CRYPTOGRAPHIC SYSTEMS ARE PROPOSED ALL THE
9 TIME BY PEOPLE WHO BELIEVE THAT THEY REPRESENT
10 SECURITY. JUST BEFORE THE START OF WORLD WAR II, A
11 MAN BY THE NAME OF EDWARD HEPBURN DEVELOPED A ROTOR
12 MACHINE, AND HE GAVE IT TO THE DEPARTMENT OF DEFENSE.
13 HE SAID "HERE, PROVE THAT IT'S GOOD. PROVE THAT IT'S
14 BAD. I WANT TO SELL THIS SYSTEM TO YOU." AND SO HE
15 WENT TO THE PEOPLE WHO WERE COMPETENT TO MAKE THIS
16 EVALUATION, AND HE CHALLENGED THEM TO MAKE THIS, AND
17 THEY CARRIED OUT THE ANALYSIS.

18 I THINK IT'S COMMON PART OF THE PRACTICE IN
19 CRYPTOGRAPHY. I MAY NOT BE ABLE TO FIND AN ARTICLE
20 THAT SAYS SUBMIT IT TO THE PATENT OFFICE THEN SUPPLY
21 IT TO THE I TRIPLE E AND THE A.M.C., THE AMERICAN
22 MATHEMATICAL COALITION, TRANSACTIONS AND WAIT TWO
23 YEARS AND SEVEN MONTHS. IF YOU DON'T SEE ANYTHING
24 THAT APPEARS IN PRINT, THEN YOU CAN GO MARKET IT. I'M
25 SURE I WILL NEVER FIND SUCH AN ARTICLE.

1 Q. YOU DID, HOWEVER, FIND THE ARTICLES THAT HAVE BEEN
2 MARKED HERE AS PLAINTIFFS' 1000 AND 1004 BY THE
3 INVENTORS THAT WE TALKED ABOUT THIS MORNING; CORRECT?

4 A. YES.

5 Q. NOW, FROM THOSE ARTICLES, THE PASSAGES YOU
6 DISCUSSED WITH HIS HONOR THIS MORNING, YOU CONCLUDED
7 THAT MR. HELLMAN AND HIS COLLEAGUES SHARE YOUR VIEW
8 THAT THERE OUGHT TO BE PRE-CERTIFICATION AND
9 PRE-TESTING OF ALGORITHMS; CORRECT?

10 A. I BELIEVE THAT THE THINGS THAT I READ OVER HERE
11 SUGGEST THAT TO MAKE A CLAIM OF COMPUTATIONAL
12 INFEASABILITY REQUIRED THE INVENTAGE OF A
13 CRYPTOGRAPHIC SYSTEM TO SUBMIT IT IN SOME FORMAL OR
14 INFORMAL WAY TO THE SCRUTINY OF THE CRYPTOGRAPHIC
15 COMMUNITY.

16 Q. AND YOU'RE AWARE FROM THE STUDY IN THIS CASE THAT
17 THAT WAS NOT DONE WITH REGARD TO THE TRAP DOOR
18 KNAPSACK BEFORE THE PATENT ISSUE; CORRECT?

19 A. WELL, IT MAY HAVE -- I DISAGREE ENTIRELY. I
20 BELIEVE THAT, WHEN THIS PAPER APPEARED IN PREPRINT
21 FORM, FOR EXAMPLE, AND WAS CIRCULATED AMONG PEOPLE IN
22 THE CRYPTOGRAPHIC COMMUNITY, PEOPLE BEGAN TO WORK ON
23 THE PROBLEM. AND SO THE PROCESS OF CERTIFICATION
24 BEGAN THE MINUTE THESE INVENTORS CAME WITH THEIR IDEA.

25 Q. YOUR TESTIMONY HERE THAT AT THE TIME THE PATENT

1 WAS APPLIED FOR IN 1977, THE TRAP DOOR KNAPSACK
2 ALGORITHM HAD BEEN SUBMITTED TO SUFFICIENT SCRUTINY
3 WITHIN THE CRYPTOGRAPHIC COMMUNITY TO PASS THE
4 COMPUTATIONALLY SECURE TEST.

5 A. NO, MAY --

6 Q. YOU'VE ANSWERED THE QUESTION.

7 A. I'M ANSWERING NO TO IT. DID IT PASS THE TEST IS
8 WHAT THE QUESTION IS. NO. THIS PAPER HIDING TRAP
9 DOOR KNAPSACKS SAYS THE MANUSCRIPT WAS RECEIVED AUGUST
10 5, 1977 BEFORE THE PATENT WAS SUBMITTED.

11 THIS PAPER IN ITS PREPRINT FORM WHICH IS THE
12 STANDARD WAY IN WHICH SCIENTIFIC MATERIAL IS
13 DISSEMINATED WAS MADE AVAILABLE TO MANY PEOPLE. THERE
14 IS NO FORMAL SUBMISSION PROCESS. THERE IS NO FORMAL
15 CERTIFYING AGENCY. IT WAS SUBMITTED. PEOPLE BEGAN TO
16 WORK ON IT.

17 Q. AND AS OF OCTOBER 6, 1977 WHEN THE PATENT
18 APPLICATION WAS FILED, THERE HAD NOT YET BEEN ADEQUATE
19 OPPORTUNITY FOR THE COMMUNITY TO DETERMINE WHETHER
20 THIS WAS A BREAKABLE SYSTEM OR NOT, HAD THERE?

21 A. THAT'S CORRECT.

22 Q. SO IN ARRIVING AT YOUR OPINION AS TO THE
23 REASONABLE MEANING TO ASCRIBE TO COMPUTATIONALLY
24 SECURE IN THIS PATENT, YOU CONCLUDED THAT THE
25 INVENTORS CHOSE A DEFINITION THAT THEY KNEW THEIR

1 PREFERRED EMBODIMENT DID NOT SATISFY; CORRECT?

2 A. COULD YOU REPEAT THE QUESTION. I'M CONFUSED AS TO
3 WHAT YOU WERE ASKING.

4 Q. YOU TRIED IN REVIEWING THE PATENT TO COME UP WITH
5 A REASONABLE INTERPRETATION OF WHAT THE INVENTORS
6 PROBABLY MEANT.

7 A. YES.

8 Q. AND THE INTERPRETATION THAT YOU CONCLUDED WAS MOST
9 REASONABLE WAS THAT THEY DEFINED COMPUTATIONALLY
10 SECURE IN A WAY THAT THEY KNEW THE EMBODIMENT IN THEIR
11 PATENT DIDN'T SATISFY; CORRECT?

12 A. I DON'T KNOW HOW TO ANSWER THAT QUESTION. THEY
13 ASSERT THAT IT WAS COMPUTATIONALLY INFEASIBLE. IN THE
14 BOARD THAT YOU HAVE PUT ON THE DISPLAY, THEY ASSERTED
15 THAT IT WAS COMPUTATIONALLY INFEASIBLE.

16 I HAVE GIVEN MY DEFINITION OF WHAT SECURE
17 MEANS. THEY HAVE USED THE WORD COMPUTATIONALLY
18 INFEASIBLE. BUT YET IN THE ARTICLE, THEY REALIZE, AND
19 THEY SAY CLEARLY "WE HAVE NOT PROVED IT'S
20 COMPUTATIONALLY INFEASIBLE."

21 Q. YOU AGREE WITH ME SOMEBODY WOULD HAVE TO BE PRETTY
22 STUPID TO PUT A DEFINITION IN A PATENT AND THEN SAY
23 ELSEWHERE IN THE PATENT "MY PREFERRED EMBODIMENT
24 DOESN'T SATISFY THAT DEFINITION"; CORRECT?

25 A. WELL, I DON'T WANT TO ACCUSE PROFESSOR HELLMAN IN

1 ANY WAY OF BEING STUPID. PROFESSOR HELLMAN SAID IN
2 THIS CLAIM IT'S COMPUTATIONALLY INFEASIBLE. IN THE
3 ARTICLE THAT WAS SUBMITTED BEFORE, HE SAYS "WE HAVE
4 NOT PROVED THAT IT IS COMPUTATIONALLY DIFFICULT FOR AN
5 OPPONENT." THOSE ARE NOT WORDS THAT I HAVE CHOSEN.
6 THAT'S WORDS THAT THE INVENTOR HAS CHOSEN.

7 I CAN'T BE HELD ACCOUNTABLE NOR WILL I MAKE A
8 JUDGMENT ABOUT HIS MOTIVES OF DOING THIS. BUT HE SAYS
9 ONE THING IN THE PATENT, AND TWO MONTHS AND ONE DAY
10 BEFORE THE PATENT WAS FILED, HE SAYS SOMETHING WHICH
11 IS CONTRADICTORY TO IT. NOW, YOU ARRIVE AT A
12 CONCLUSION.

13 Q. THERE ARE REALLY JUST TWO ALTERNATIVES. EITHER
14 HE'S JUST PLAIN STUPID OR HE'S TRYING TO PRACTICE
15 FRAUD IN THE PATENT OFFICE. THAT KIND OF EXHAUSTS IT,
16 DOESN'T IT?

17 A. LISTEN, I'M NOT A LAWYER AS YOU'VE ALREADY TOLD
18 THE COURT. HOW AM I TO ARRIVE AT A DECISION?

19 Q. YOU HOLD A PATENT YOURSELF, DON'T YOU?

20 A. I DO?

21 Q. SO YOU'RE NOT TOTALLY UNFAMILIAR WITH THE PATENT
22 PROCESS.

23 A. I'M NOT UNFAMILIAR WITH THE PATENT PROCESS.

24 Q. AND BASED ON YOUR ADMITTEDLY NOT A LAWYER BUT
25 NONETHELESS FAMILIARITY WITH THE PROCESS, CAN YOU

1 THINK OF WAY THAT MR. HELLMAN COULD HAVE USED THE
2 DEFINITION OF COMPUTATIONALLY SECURE THAT YOU'RE
3 ASKING THIS COURT TO ADOPT UNLESS HE WAS EITHER
4 ABJECTLY STUPID OR TRYING TO DEFRAUD THE PATENT
5 OFFICE?

6 A. I WILL ABSOLUTELY NOT MAKE EITHER OF THOSE
7 JUDGMENTS. THAT'S SOMETHING FOR THE COURT TO MAKE.
8 THAT'S SOMETHING FOR THE COURT TO DECIDE AS TO WHETHER
9 HE WAS BEING DUPLICITOUS OR STUPID OR WHATEVER
10 ALTERNATIVE THE COURT WILL HAVE.

11 IT'S NOT A DECISION FOR ME. I CAN ONLY READ
12 WHAT HE SAYS IN THE ARTICLE, MR. KENNEDY, AND I CAN
13 ONLY LOOK AT WHAT HE SAYS IN THE PATENT. THERE ARE
14 CONTRADICTORY STATEMENTS. I THINK I'VE SAID IT.

15 Q. LET'S MOVE ON. I AGREE. CAN YOU POINT US TO
16 ANYTHING IN WRITING AS TO OCTOBER 6, 1977 WHEN THE
17 PATENT APPLICATION WAS FILED THAT DESCRIBED HOW ONE
18 WOULD BREAK A TRAP DOOR KNAPSACK?

19 A. WELL, I THINK THAT NO ONE BEFORE OCTOBER 6, 1977
20 OR AUGUST 5, 1977 WHICHEVER DATE YOU WISH HAD USED THE
21 TERM TRAP DOOR KNAPSACK. SO YOU WOULD NOT SEE THE
22 TERM TRAP DOOR KNAPSACK APPEARING IN AN ARTICLE. THE
23 METHODS USED TO BREAK THE CRYPTOGRAPHIC SYSTEM HAD
24 BEEN PUBLISHED. VARIOUS METHODS HAVE BEEN PUBLISHED
25 BY PEOPLE BEFORE THEN.

1 THE METHODS THAT ARE USED TO BREAK ACTUALLY
2 THE TRAP DOOR KNAPSACK PROBLEM ARE MATHEMATICAL
3 METHODS THAT HAVE BEEN KNOWN FOR A LONG TIME. THE WAY
4 THAT YOU PACKAGE THEM TOGETHER, THE WAY THAT YOU PUT
5 THEM TOGETHER TO SOLVE THIS PROBLEM, THAT OF COURSE
6 REPRESENTS THE CREATIVITY OF THE PERSON WHO HAS BROKEN
7 THE KNAPSACK SYSTEM BUT IT'S NOT --

8 Q. GO AHEAD.

9 A. I THINK I FINISHED.

10 Q. ISN'T IT FACT THAT YOU TOLD US YESTERDAY THAT IT
11 WASN'T UNTIL 1982, YEARS AFTER THE PATENT WAS APPLIED
12 FOR AND TWO YEARS AFTER IT WAS ISSUED THAT MR. SHAMIR
13 FIRST PUBLISHED A WAY OF BRAKING THE SIMPLEST
14 KNAPSACK; CORRECT?

15 MR. HASLAM: OBJECT TO THE QUESTION, YOUR
16 HONOR. I THINK MR. KENNEDY IS THE ONE THIS MORNING
17 THAT OBJECTED AND SAID THAT THEY WERE NOT AS SECURE
18 AND WHETHER IT HAD BEEN BROKEN WAS A QUESTION THAT
19 WENT BEYOND THE BOUNDS HERE.

20 THE COURT: REPEAT THE QUESTION, PLEASE.

21 MR. KENNEDY: IT WASN'T BEFORE 1982 THAT THE
22 FIRST PUBLISHED ARTICLE ABOUT BREAKING A KNAPSACK WAS
23 PUT OUT.

24 THE COURT: OVERRULED.

25 THE WITNESS: I AGREE. IN 1982 THE FIRST --

1 MR. KENNEDY: Q. DO YOU HAVE A COPY OF THE
2 PATENT UP THERE IN FRONT OF YOU?

3 A. YES, I DO.

4 Q. MAY I DIRECT YOUR ATTENTION TO COLUMN 5, LINES 1
5 THROUGH 15. OF COURSE THIS WAS PART OF WHAT YOU READ
6 IN ARRIVING AT YOUR OPINIONS IN THIS CASE; CORRECT?

7 A. YES, I'M FAMILIAR WITH THIS MATERIAL.

8 Q. AND YOU TOOK THIS INTO ACCOUNT IN ARRIVING AT YOUR
9 DEFINITION?

10 A. I TOOK THE HI-LIGHTED MATERIAL WHICH DEFINES --
11 GIVES THE INVENTOR'S DEFINITION OF COMPUTATIONALLY
12 INFEASIBLE.

13 Q. AND FROM READING THAT LANGUAGE, DIDN'T YOU ARRIVE
14 AT THE OPINION THAT BY COMPUTATIONALLY INFEASIBLE,
15 THEY MEANT UNBROKEN GIVEN CURRENT KNOWLEDGE AND
16 METHODS?

17 A. NO.

18 Q. AS YOU STARTED READING THAT PARAGRAPH AND YOU GOT
19 TO THE THIRD LINE WHERE IT SAID "BUT TO THE BEST OF
20 CURRENT KNOWLEDGE, FINDING A SOLUTION REQUIRES A
21 NUMBER OF OPERATIONS WHICH GROW EXPONENTIALLY." DID
22 YOU GIVE THAT STATEMENT ANY WEIGHT IN ARRIVING AT YOUR
23 OPINION IN THIS CASE?

24 A. NO, BECAUSE I'M LOOKING FOR THE DEFINITION OF
25 COMPUTATIONALLY INFEASIBLE. AT THE HI-LIGHTED

1 MATERIAL THEY SAY "DEFINITION, A TASK IS
2 COMPUTATIONALLY INFEASIBLE IF." SO THEY DEFINE
3 COMPUTATIONALLY INFEASIBLE. BUT WHAT PROFESSOR
4 HELLMAN AND MR. MERKEL DID IS DESCRIBE THE CURRENT
5 STATE OF THE ART AT THE TIME OF ALGORITHMS TO SOLVE
6 THE KNAPSACK PROBLEM.

7 Q. SO WHAT YOU FOCUSED IN ON WAS THE HI-LIGHTED LAST
8 SENTENCE IN COLUMN 5, LINES 1 THROUGH 15; CORRECT?

9 A. THAT'S RIGHT.

10 Q. THE ONE THAT ENDS WITH THE WORDS "EXISTING
11 COMPUTATIONAL METHODS AND EQUIPMENT"; CORRECT?

12 A. YES. BUT I BELIEVE YOU ARE READING IT OUT OF
13 CONTEXT.

14 Q. WELL, LET'S READ THE WHOLE SENTENCE.

15 A. MAY I READ IT?

16 Q. SURE, WE'LL LET YOU GO.

17 A. "A TASK IS COMPUTATIONALLY INFEASIBLE IF ITS COST
18 IS MEASURED BY EITHER THE AMOUNT OF MEMORY USED OR THE
19 COMPUTING TIME IS FINITE BUT IMPOSSIBLY LARGE."

20 WELL, THEY NOW WANT TO SAY WHAT IMPOSSIBLY
21 LARGE IS. THEY SAY, "FOR EXAMPLE, ON THE ORDER OF
22 APPROXIMATELY 10 TO THE 30TH OPERATIONS." BUT
23 OPERATIONS IS NOT TIME. OPERATIONS IS SOME OTHER
24 UNIT. SO NOW THEY HAVE GOT TO TRANSLATE WHICH MEAN
25 THE WORD OPERATIONS AND TIME, AND THEN THEY TELL US

1 HOW TO DO IT.

2 THEY SAY TAKE THE EXISTING COMPUTATIONAL
3 METHODS AND EQUIPMENT AS OF THE DATE OF FILING OF THE
4 PATENT OCTOBER 6, 1977. HOW LONG WILL 10 TO THE 30TH
5 OPERATIONS TAKE? AND I'VE MADE THAT CONVERSION, AND I
6 FIND THE 10 TO THE 30TH OPERATIONS IS A VERY LONG
7 TIME.

8 Q. YOU DID TAKE EXISTING COMPUTATIONAL METHODS AND
9 EQUIPMENT INTO ACCOUNT?

10 A. YES, YES.

11 Q. CAN I ALSO DIRECT YOUR ATTENTION BACK TO COLUMN 2,
12 LINES 43 THROUGH 47.

13 I'M SORRY. I DON'T HAVE A BLOW UP OF THIS,
14 YOUR HONOR, BUT IT'S COLUMN 2, 43 THROUGH 47.

15 THE COURT: OKAY.

16 MR. KENNEDY: Q. AND THE SENTENCE READING
17 "THE ILLUSTRATED EMBODIMENT DIFFERS FROM PRIOR
18 APPROACHES TO A PUBLIC KEY CRYPTOSYSTEM AS DESCRIBED
19 IN MULTIUSER CRYPTOGRAPHIC TECHNIQUES IN THAT IT IS
20 BOTH PRACTICAL TO IMPLEMENT AND IS DEMONSTRABLY
21 INFEASIBLE TO INVERT USING KNOWN METHODS."

22 DID YOU READ THAT AND TAKE THAT INTO ACCOUNT
23 IN ARRIVING AT YOUR OPINION?

24 A. I WILL TAKE THAT INTO ACCOUNT IF I KNEW WHAT THE
25 AUTHORS MEANT BY THE WORD "INFEASIBLE," AND I HAVE TO

1 READ LATER. I HAVE TO READ FURTHER ON TO COLUMN 5 TO
2 SEE WHAT INFEASIBLE MEANS, AND THAT'S WHAT I'VE DONE.
3 Q. AND GOING BACK TO CLAIM ONE, YOU TOLD US THIS
4 MORNING THAT IT'S YOUR OPINION THAT THE WORD
5 GENERATING DOESN'T HAVE A WELL-UNDERSTOOD MEANING IN
6 THE ART; CORRECT?

7 A. ABSOLUTELY.

8 Q. IN ARRIVING AT THE OPINION AND GIVING THAT
9 TESTIMONY, WHAT DID YOU DO TO GO TRY TO FIND OUT
10 WHETHER GENERATING DID OR DID NOT HAVE A
11 WELL-UNDERSTOOD MEANING?

12 A. WELL, I USED MY SKILL IN THE ART, MY KNOWLEDGE OF
13 CRYPTOGRAPHY. IF YOU TAKE, FOR EXAMPLE, A BOOK LIKE
14 SNEERS AND LOOK AT THE INDEX AND SEE IF CAN I FIND THE
15 WORD GENERATING, I DON'T THINK YOU'RE GOING TO FIND
16 THE WORD GENERATING. I MIGHT FIND GENERATING THE
17 SYMMETRIC GROUP. WHEN I LOOK AT THAT WORD, IT'S
18 INDEFINITE. IT DOESN'T TELL ME. IT SAYS "GENERATED
19 FROM SAID RANDUM NUMBERS A SECRET DECIPHERING KEY."

20 SO I KNOW WHAT THE AUTHORS INTEND. THEY
21 INTEND FOR ME TO TAKE THESE RANDUM NUMBERS AND PRODUCE
22 FROM THOSE RANDUM NUMBERS A SECRET DECIPHERING KEY,
23 BUT I DON'T KNOW HOW THEY INTEND TO DO IT. I HAVE NO
24 WAY. IT'S TOO INDEFINITE FOR ME TO FIGURE OUT WHAT
25 THE AUTHORS INTENDED JUST UPON THE BASIS OF THOSE

1 WORDS.

2 AND, FOR EXAMPLE, I SEE THE WORD PROCESSING
3 APPEARING TWICE ON THIS CHART OVER HERE. IT'S
4 PROCESSING THE MESSAGE, AND THE OTHER IS PROCESSING
5 THE ENCIPHERED MESSAGE. THE WORD PROCESSING IS NOT
6 DOING THE SAME THING BOTH TIMES. YOU HAVE TO READ THE
7 ENTIRE THING IN CONTEXT TO UNDERSTAND WHAT THE --
8 ATTEMPT TO UNDERSTAND WHAT THE AUTHORS, THE INVENTORS
9 OF THIS PATENT INTEND.

10 Q. DO YOU REMEMBER WHAT QUESTION YOU'RE ANSWERING?

11 A. YOU'VE ASKED ME IF I UNDERSTOOD WHAT GENERATING
12 MEANT.

13 Q. I ASKED YOU WHAT YOU DID TO ARRIVE AT YOUR
14 OPINION.

15 A. MY TECHNICAL EXPERTISE, MY KNOWLEDGE OF
16 CRYPTOGRAPHY.

17 Q. AND YOU TOLD US YOU LOOKED AT ONE BOOK; CORRECT?

18 A. I DIDN'T LOOK AT THAT -- I'VE LOOKED AT THAT
19 BOOK. I DON'T THINK I'VE LOOKED FOR THE WORD
20 GENERATING IN THE INDEX.

21 Q. DID YOU TRY LOOKING IN A DICTIONARY?

22 A. OH, YES. I DON'T THINK I LOOKED AT A DICTIONARY,
23 BUT I LOOKED UP WORDS IN DICTIONARIES.

24 Q. WELL, BEFORE COMING HERE AND SAYING THAT
25 GENERATING DIDN'T HAVE AN ACCEPTED MEANING IN THE ART,

1 DID YOU DOUBLE CHECK TO SEE, IF MAYBE PEOPLE WENT TO
2 DICTIONARIES, THEY'D FIND OUT IN MATHETMATICS
3 GENERATING DOES HAVE AN UNDERSTOOD MEANING? DID YOU
4 DO THAT?

5 A. NO, I DID NOT DO THAT.

6 MR. KENNEDY: YOUR HONOR, EXHIBIT 50004 --
7 SORRY, I'M THINKING BIG NUMBERS HERE. 504 IS A
8 PORTION OF WEBSTER'S THIRD NEW INTERNATIONAL
9 DICTIONARY, 1981, PAGE 945.

10 Q. I WOULD DIRECT THE WITNESS'S ATTENTION IN
11 PARTICULAR TO DEFINITION NUMBER THREE OF GENERATE TO
12 DEFINE AS A "MATHEMATICAL OR LINGUISTIC SET OR
13 STRUCTURE BY THE APPLICATION OF ONE OR MORE RULES OR
14 OPERATIONS TO GIVE IN QUANTITIES." DOES THAT IN ANY
15 WAY AFFECT YOUR OPINION?

16 A. COULD YOU EXCUSE ME. I'D LIKE TO GET MY READING
17 GLASSES.

18 Q. I APOLOGIZE. SORRY, DOCTOR.

19 A. OKAY. NOW, YOU WERE USING DEFINITION --

20 Q. NUMBER THREE.

21 A. GENERATING. I'M LOOKING AT GENERATION. LET'S
22 LOOK AT GENERATING.

23 Q. IT'S UNDER GENERATE, PROFESSOR.

24 A. TO DEFINE THIS "IN MATHEMATICAL OR LINGUISTIC SET
25 OR STRUCTURE BY THE APPLICATION OF ONE OR MORE RULES

1 OF OPERATIONS TO GIVE IN QUANTITIES." FOR EXAMPLE, I
2 JUST READ THAT.

3 Q. AND THAT DOESN'T IN ANY WAY AFFECT ANY OPINION
4 THAT YOU'VE EXPRESSED HERE THAT GENERATING HAS NO
5 ACCEPTED MEANING WITHIN THE ART; CORRECT?

6 A. I MAINTAIN WHAT I HAVE SAID. IT TELLS YOU WHAT
7 YOU WANT TO DO, BUT IT DOESN'T GIVE YOU ANY INDICATION
8 AS TO WHAT YOU WERE TO DO.

9 ALL THIS DEFINITION IS TO SAY THE APPLICATION
10 OF ONE OR MORE RULES OR OPERATIONS THAT IS TO DO
11 SOMETHING TO A GIVEN QUANTITY. I'M WILLING TO ACCEPT
12 THE DEFINITION OF THIS DICTIONARY OVER HERE, BUT IT
13 DOESN'T TELL ME ANYTHING DIFFERENT THAN WHAT I'VE READ
14 ON THE BOARD.

15 IT SAYS RANDUM NUMBERS ARE TO BE USED TO GET
16 SOMETHING ELSE, A SECRET DECIPHERING KEY. BUT IT
17 DOESN'T TELL ME, YOU KNOW, ANY SORT OF MATHEMATICAL
18 OPERATION WHICH TAKES INPUT AND PRODUCED AN OUTPUT CAN
19 BE THOUGHT OF AS GENERATING.

20 SO THIS IS DESCRIBING A VERY GENERAL
21 OPERATION WHERE YOU TAKE ANY KIND OF RANDUM NUMBERS
22 AND GET SOMETHING ELSE IS AN EXAMPLE OF GENERATING.
23 THIS DOESN'T TELL ME. THIS IS A DESCRIPTION OF AN ACT
24 OF WHAT THE INVENTORS INTENDED, BUT IT DOESN'T TELL ME
25 EXACTLY HOW THEY WANTED TO DO IT OR EVEN GIVE ANY

1 GUIDANCE TO THAT.

2 Q. SO YOUR OPINION IS STILL THE SAME AS IT WAS THIS
3 MORNING?

4 A. THE SAME AS IT WAS A FEW MINUTES AGO.

5 Q. AND I ASSUME YOUR OPINION AS TO PROCESS IS THE
6 SAME AS IT WAS THIS MORNING THAT THAT HAS NO
7 RECOGNIZABLE ACCEPTANCE IN THE ART?

8 A. IN THE CRYPTOGRAPHIC ART, IT HAS NO MEANING. I'M
9 SURE THAT YOU HAVE FOUND FOR ME THE WORD PROCESSING
10 OVER HERE.

11 Q. NO.

12 A. YOU HAVEN'T?

13 Q. JUST BEAR WITH ME. I'VE GOT AN EQUALLY GOOD
14 APPROACH ON THIS ONE, BEAR WITH ME. IT'S GOING TO BE
15 DIFFERENT.

16 IN PREPARING TO COME HERE AND GIVE YOUR
17 TESTIMONY, DID YOU CHECK WITH ANY OF YOUR FELLOW
18 EXPERTS SUCH AS DUSSE FROM RSA, THE GOOD LOOKING
19 GENTLEMAN WITH A CREW CUT SITTING BACK HERE, TO SEE IF
20 HE AGREED WITH YOU THAT PROCESSING DOESN'T HAVE A
21 RECOGNIZED MEANING IN THE ART? DID YOU DO THAT?

22 A. NO, I MET MR. DUSSE THIS MORNING.

23 Q. DID YOU CHECK WITH ANYBODY ELSE THAT YOU
24 CONSIDERED EXPERIENCED IN THE ARTS SUCH AS, FOR
25 EXAMPLE, MR. SCHLAFLY TO SEE IF HE AGREED WITH YOUR

1 VIEW?

2 A. NO, I DID NOT CHECK WITH HIM.

3 Q. I WANT YOU TO ASSUME HYPOTHETICALLY THAT, WHEN
4 MR. DUSSE WAS DEPOSED AS AN EXPERT IN THIS CASE A
5 COUPLE WEEKS AGO, HE HAD NO TROUBLE DEFINING
6 PROCESSING AND TOLD US, "IN THE CONTEXT OF A DIGITAL
7 SIGNATURE PROCESSOR, PROCESSING IS THE ACT OF
8 TRANSFORMING DIGITAL SIGNALS OR MANIPULATING DIGITAL
9 SIGNALS."

10 ASSUMING -- AND WE'LL TIE IT UP -- THAT THAT
11 WAS MR. DUSSE'S TESTIMONY, AND HE'LL BE HERE LATER
12 THIS AFTERNOON, DOES THAT AFFECT YOUR OPINION AT ALL
13 THAT PROCESSING DOESN'T HAVE A RECOGNIZED MEANING IN
14 THE ART?

15 MR. HASLAM: OBJECT TO THE QUESTION AS
16 LACKING FOUNDATION. I ALSO THINK THE FOUNDATION IS
17 NOT AS TO WHETHER IT WAS TESTIFIED TO. I DON'T THINK
18 THEY HAVE ESTABLISHED OR CAN ESTABLISH THAT THE '582
19 PATENT DISCLOSED A PROCESS THAT THE WITNESS WAS
20 REFERRING TO.

21 THE COURT: YOU'RE TALKING ABOUT THE WORD
22 PROCESSING; CORRECT?

23 MR. KENNEDY: CORRECT.

24 THE COURT: THE CONTEXT OF --

25 MR. KENNEDY: MR. DUSSE WAS ASKED ABOUT

1 PROCESSING IN THE CONTEXT OF THE CLAIMS IN THIS CASE.
2 AGAIN, THE DEPOSITION TESTIMONY SPEAKS FOR ITSELF.
3 WE'LL HAVE HIM ON THE STAND HERE THIS AFTERNOON.

4 I'M REPRESENTING AS AN OFFICER OF THE COURT
5 IT WAS GIVEN. ALL I WANT TO FIND OUT NOW IS WHETHER,
6 EVEN IF ANOTHER OF HIS SAME CLIENT'S EXPERTS HAS A
7 DIFFERENT VIEW, THAT HAS ANY EFFECT ON THIS
8 GENTLEMAN'S OPINION. I THINK I KNOW HIS ANSWER.

9 THE COURT: OBJECTION OVERRULED.

10 THE WITNESS: MY OPINION IS THE SAME. WHEN I
11 LOOK AT THE WORDS "PROCESSING THE MESSAGE" AS IN THE
12 FIRST, SECOND, THIRD, FOURTH, FIFTH, AND IN THE
13 SEVENTH PART OF THE CLAIM ONE, "PROCESSING THE
14 ENCIPHERED MESSAGE," IT DESCRIBED TO ME WHAT IS TO BE
15 DONE, BUT IT DOESN'T DESCRIBE TO ME HOW IT'S BEING
16 DONE. IT DESCRIBES THE ACTS BUT NOT THE METHOD AT
17 ALL.

18 Q. IT WOULDN'T MATTER HOW MANY CRYPTOANALYSTS OR
19 COMPUTER SPECIALISTS OR MATHEMATICIANS GOT UP HERE AND
20 SAY, "YES, IT DOES HAVE AN ACCEPTED MEANING," YOUR
21 OPINION WOULD STILL BE THAT IT DOESN'T; CORRECT?

22 A. WELL, YOU'VE ONLY OFFERED ONE, MR. DUSSE. I STAND
23 ON WHAT I SAID. THAT LANGUAGE OVER THERE IS VAGUE AND
24 INDEFINITE. IT DOES NOT SAY -- GIVE GUIDANCE TO WHAT
25 THE INVENTION IS.

1 Q. AND DID YOU DO ANY KIND OF REALITY CHECK IN
2 CONSULTING WITH OTHER PEOPLE BEFORE EXPRESSING THE
3 OPINION TO SEE IF THERE WERE OTHER FOLKS WHO SHARED
4 YOUR VIEW?

5 A. NO, I DID NOT DO ANY REALITY CHECKS.

6 Q. I WILL DIRECT YOUR ATTENTION NEXT TO CLAIM TWO OF
7 THE PATENT. AGAIN, I'M SORRY WE DON'T HAVE A BLOW UP
8 OF THAT. DO YOU HAVE THE --

9 A. YES, I DO.

10 Q. AS I UNDERSTAND IT, YOUR VIEW IS THAT THE WORD
11 AUTHENTICATION AS USED IN THERE MEANS THAT YOU'RE
12 ACTUALLY VERIFYING THE IDENTITY OF THE PERSON WITH
13 WHOM YOU'RE COMMUNICATING.

14 A. THAT'S CORRECT.

15 Q. NOW, CAN YOU POINT US TO ANY AGAIN BOOK, TREATISE,
16 ARTICLE, OR WHATEVER THAT SAYS AUTHENTICATION MEANS
17 NOT JUST THAT SOMEBODY HAS STOLEN THE KEY, HAS THE
18 ENCIPHERING MACHINE, HAS SOMEHOW GOTTEN ACCESS TO IT,
19 BUT THAT IT'S ACTUALLY THE LIVE HUMAN BEING THAT YOU
20 THINK YOU'RE TALKING TO?

21 A. IF YOU WILL GIVE ME A SECOND. I THOUGHT I GAVE
22 YOU THIS MORNING --

23 Q. HOW ABOUT COLUMN 18, LINES 46, "THE PUBLIC
24 DEPOSITORY"?

25 A. WELL, THERE'S -- I'M LOOKING FOR AN EVEN MORE

1 BASIC ROTATION. IF YOU WILL GIVE ME A MINUTE, I WILL
2 TRY TO FIND IT. I BELIEVE IT'S IN "NEW DIRECTIONS,"
3 BUT LET ME CHECK. NO, IN THE PAPER "TRAP DOOR
4 KNAPSACKS," WHICH IS EXHIBIT 1003, ON PAGE 527, THE
5 LAST LINE USES THE WORD "HE COULD IDENTIFY," AND THEN
6 HE PUTS IN PARENTHESIS "AUTHENTICATE." I INTERPRET
7 THAT TO MEAN THAT AUTHENTICATION IS CONNECTED WITH
8 IDENTIFICATION.

9 Q. SO IT'S YOUR UNDERSTANDING THAT IN THE ART TO
10 AUTHENTICATE MEANS TO ELIMINATE ANY POSSIBILITY OF AN
11 IMPOSTOR, BUT IT HAS TO BE THE REAL PERSON; IS THAT
12 CORRECT?

13 A. THAT IS ABSOLUTELY CORRECT.

14 Q. HOW COULD WE AUTHENTICATE THAT YOU ARE PROFESSOR
15 KONHEIM?

16 A. YOU COULD AUTHENTICATE THAT I AM PROFESSOR KONHEIM
17 OR ALAN KONHEIM BY ASKING ME TO PRODUCE MY DRIVER'S
18 LICENSE.

19 Q. HOW DO I KNOW IT'S NOT A FORGERY? YOU COULD BUY
20 THOSE THINGS FOR 500 BUCKS.

21 A. WELL, THEN IT'S UP TO YOU TO SAY, "HEY, THAT'S A
22 FORGERY."

23 Q. OTHER THAN IF YOU COULD TRANSMIT DNA OVER COMPUTER
24 WIRES, CAN YOU THINK OF ANY WAY OF AUTHENTICATING THE
25 IDENTITY OF SOMEBODY IN THE WAY YOU'RE TALKING ABOUT?

1 A. SUPERMARKETS ACCEPT MY DRIVER'S LICENSE AS PROOF
2 OF MY IDENTITY. IF YOU WISH, I'LL HAVE MY PASSPORT
3 FEDEXED UP HERE.

4 Q. YOU TOLD US THIS MORNING THAT HAVING THE SECRET
5 KEY WASN'T ENOUGH FOR AUTHENTICATION.

6 A. THAT'S RIGHT BECAUSE THE SECRET KEY IS NOT
7 CONNECTED WITH MY IDENTITY. YOU MUST FIND SOMETHING
8 THAT LINKS THE SECRET KEY AND THE IDENTITY. AFTER
9 ALL, CLAIM TWO SAYS THAT THE TRANSMITTER USES THE --
10 GETS THE PUBLIC KEY FROM THE RECEIVER AND THEN
11 ENCIPHERS INFORMATION.

12 THE TRANSMITTER DOESN'T KNOW THAT IT'S
13 DEALING WITH ALAN KONHEIM. IT'S DEALING WITH SOMEONE
14 WHO WAS GIVEN THE PUBLIC KEY.

15 Q. THE SAME WAY YOU GO INTO SAFEWAY AND SHOW YOUR
16 DRIVER'S LICENSE. THEY DON'T KNOW FOR SURE THEY'RE
17 DEALING WITH PROFESSOR KONHEIM. HOW DO THEY KNOW IT'S
18 YOU?

19 A. THEY SEE MY PICTURE ON IT.

20 Q. HOW DO THEY KNOW ITS NOT ANOTHER SHORT GOOD
21 LOOKING GUY THAT'S ON THERE?

22 A. THERE IS NO ONE AS GOOD LOOKING AS ME EVEN IF I'M
23 NOT A LAWYER.

24 Q. AND DIRECTING YOUR ATTENTION BACK TO COLUMN 18,
25 THE PORTION WE WERE TALKING ABOUT THIS MORNING AGAIN

1 IT WAS LINES 47 -- 46 THROUGH WHERE THE CLAIMS START.

2 A. YES.

3 Q. THAT TALKS ABOUT AN ALTERNATIVE VARIATION UNDER
4 WHICH KEYS COULD BE REGISTERED WITH SOME KIND OF A
5 SYSTEM TO INCREASE THEIR RELIABILITY; CORRECT?

6 A. THAT'S QUITE CORRECT.

7 Q. AND THAT'S BEING PROPOSED -- AS IT STARTS AT LINE
8 46, "VARIATIONS ON THE ABOVE-DESCRIBED EMBODIMENT ARE
9 POSSIBLE." IT SAYS THAT, DOESN'T IT?

10 A. YES, IT DOES.

11 Q. SO THE IDEA OF FILING SOMETHING IN A DEPOSITORY IS
12 NOT PART OF THE ACTUAL EMBODIMENT THAT'S PROPOSED IN
13 THE PATENT, IS IT.

14 A. IT IS NOT.

15 Q. AND ONCE AGAIN, IN ORDER FOR YOUR DEFINITION OF
16 AUTHENTICATION TO BE CORRECT, WE'VE GOT TO ASSUME THAT
17 THE INVENTORS PROPOSED A DEFINITION THAT THEIR OWN
18 PREFERRED EMBODIMENT DID NOT SATISFY; CORRECT?

19 A. WELL, I THINK YOU HAVE TO READ ON COLUMN ONE "AN
20 AUTHENTICATION SYSTEM PREVENTS THE UNAUTHORIZED
21 INJECTION OF MESSAGES INTO AN INSECURE CHANNEL
22 ASSURING THE RECEIVER OF THE MESSAGE OF THE LEGITIMACY
23 OF THE SENDER."

24 WHAT THEY ARE TALKING ABOUT HERE BY SAYING
25 "VARIATIONS OF," THEY SAY IN ADDITION TO THE SYSTEM

1 THAT WE ARE PROPOSING, YOU CAN DO THE FOLLOWING
2 ADDITIONAL FACTS. YOU CAN TAKE THE PUBLIC KEY AND
3 REGISTER IT BY GOING IN AND OFFERING THE PUBLIC KEY,
4 YOUR LICENSE, YOUR FINGERPRINTS, MAYBE YOUR DNA AS
5 PROOF THAT THAT PUBLIC KEY BELONGS TO RAOUL KENNEDY.

6 AND THEREFORE, WHEN YOU OFFER YOUR PUBLIC KEY
7 TO BOB FRAM, THEN BOB FRAM CAN CHECK THE DEPOSITORY
8 AND SEE THAT HE HAS RECEIVED THE KEY FROM RAOUL
9 KENNEDY. THEREFORE, WHEN HE IS IN COMMUNICATION WITH
10 YOU, HE KNOWS HE IS DEALING WITH YOU AND NOT SOME
11 IMPOSTER.

12 Q. PROFESSOR KONHEIM, UNDER YOUR DEFINITION OF
13 AUTHENTICATION, THE PREFERRED EMBODIMENT IN THE PATENT
14 DOESN'T SATISFY IT, DOES IT.

15 A. NO, IT DOES NOT SATISFY IT.

16 MR. KENNEDY: THANK YOU. I HAVE NO FURTHER
17 QUESTIONS. THANK YOU VERY MUCH.

18 MR. HASLAM: YOUR HONOR, I HAVE AN OBJECTION
19 TO MR. FLINN QUESTIONING ON THIS GROUND. SINCE THE
20 BEGINNING OF THIS CASE, ALL THE DEFENDANTS IN THE CASE
21 HAVE FILED JOINT RESPONSES -- CYLINK, C.K.C., AND
22 STANFORD. I THINK THIS IS AN ATTEMPT TO TAKE TWO
23 SHOTS AT THE SAME WITNESS.

24 I DON'T SEE ANY REASON WHY, WHY IF THEY HAVE
25 BEEN ABLE TO FILE JOINT PAPERS AT THE BEGINNING OF THE

1 CASE, WE NEED ESSENTIALLY THE SAME SIDE QUESTIONING
2 THE WITNESS.

3 THE COURT: WELL, ADDITIONAL QUESTIONS, DON'T
4 GO OVER THE SAME QUESTIONS.

5 MR. FLINN: THEY WILL BE DIFFERENT QUESTIONS,
6 YOUR HONOR.

7 THE COURT: OKAY.

8 CROSS-EXAMINATION

9 BY MR. FLINN: Q. DR. KONHEIM, HAVE YOU EVER
10 HEARD OF A BOOK CALLED "THE CODE BREAKERS" WRITTEN BY
11 ONE DAVID KANN?

12 A. YES, I HAVE.

13 Q. HAVE YOU READ IT?

14 A. YES, I HAVE.

15 Q. WHAT IS THE BOOK ABOUT?

16 A. THE BOOK IS ABOUT THE HISTORY OF CRYPTOGRAPHY.

17 Q. IS THIS A PRETTY WELL-KNOWN BOOK IN THE ART?

18 A. YES, IT CERTAINLY IS.

19 Q. WOULD YOU AGREE THAT THE AUTHOR, DAVID KANN, IS A
20 RECOGNIZED AUTHORITY IN THAT AREA?

21 A. WELL, I WOULD -- DAVID KANN IS NOT A
22 CRYPTOGRAPHER. DAVID KANN IS A REPORTER.

23 Q. I MEAN IN THE HISTORY OF CRYPTOLOGY AS OPOSED TO
24 CRYPTOGRAPHY ITSELF.

25 A. HE IS A VERY KNOWLEDGEABLE PERSON IN THE HISTORY

1 OF CRYPTOGRAPHY.

2 Q. NOW, AS OF 1977 YOU WERE ALREADY WELL INVOLVED IN
3 THE FIELD OF CRYPTOGRAPHY; IS THAT RIGHT?

4 A. THAT'S CORRECT.

5 Q. SO YOU'D BE PRETTY FAMILIAR WITH THE USE OF THE
6 TERMS IN THE FIELD OF CRYPTOGRAPHY IN 1977; IS THAT
7 CORRECT?

8 A. I BELIEVE I WOULD BE.

9 Q. AND YOU'VE BEEN IN A PRETTY GOOD POSITION TO SEE
10 THE FIELD ON A FAIRLY CONSTANT BASIS FROM 1977 TO THE
11 PRESENT. IS THAT FAIR?

12 A. THAT'S CORRECT.

13 Q. NOW, YOU'VE TESTIFIED A LOT TODAY ABOUT HOW
14 VARIOUS TERMS ARE USED IN THE ART. HAS THERE BEEN A
15 SUBSTANTIAL CHANGE IN THE MEANING OF TERMS FROM 1977
16 TO THE PRESENT?

17 A. WELL, I'M NOT SURE THAT SOME TERMS MAY HAVE
18 CHANGED THE MEANING.

19 Q. ANY TERMS THAT WE'VE BEEN USING TODAY THAT YOU CAN
20 IDENTIFY MEAN SOMETHING DIFFERENTLY THAN THEY DID IN
21 1977?

22 A. NO, NONE THAT I CAN POINT TO.

23 Q. YESTERDAY, YOU USED THE TERM -- AND I WANT TO JUST
24 SEE IF I CAN UNDERSTAND IT -- NUMBER THEORY OR NUMBER
25 THEORIST. DO YOU RECALL THAT?

1 A. YES.

2 Q. WHAT IS THAT?

3 A. NUMBER THEORY IS A BRANCH OF MATHEMATICS THAT
4 DEALS WITH PROBLEMS WHERE THE SOLUTIONS ARE INDICES AS
5 OPPOSED TO REAL NUMBERS AND WHERE RATIONAL NUMBERS AND
6 TRANSINDENTIAL NUMBERS LIKE π AND e , NUMBER THEORY
7 DEALS WITH THE PROPERTIES OF INDICES.

8 Q. IS NUMBER THEORY RELEVANT TO CRYPTOGRAPHY?

9 A. YES, NUMBER THEORY IS VERY RELEVANT TO CRYPTOLOGY.

10 Q. IS NUMBER THEORY RELEVANT TO THE SECURITY OF
11 CRYPTOGRAPHY?

12 A. IT'S RELEVANT TO CRYPTOGRAPHY AND ALL THINGS
13 CONNECTED WITH CRYPTOLOGY.

14 Q. WOULD AN EXPERT IN NUMBER THEORY IN YOUR VIEW BE
15 AN APPROPRIATE PERSON TO APPLY ON CRYPTOGRAPHIC
16 TECHNOLOGY?

17 A. WOULD I ACCEPT A DEFINITION FROM SOMEONE WHO IS A
18 NUMBER THEORIST? I MIGHT.

19 Q. THIS MORNING YOU TALKED ABOUT SOMETHING CALLED DES
20 OR D.E.S.; IS THAT RIGHT?

21 A. YES.

22 Q. NOW, THAT WAS THE NAME THAT WAS GIVEN A
23 CRYPTOGRAPHIC SYSTEM. IT'S A SYMMETRIC, A NON-PUBLIC
24 KEY SYSTEM; CORRECT?

25 A. CORRECT.

1 Q. AND IT DOMINATED THE ENCRYPTION STANDARD ONCE IT
2 BECAME A FEDERAL STANDARD; RIGHT?

3 A. I THINK SO.

4 Q. IT WAS NOT CALLED DIGITAL ENCRYPTION STANDARD
5 UNTIL IT BECAME A DIGITAL ENCRYPTION STANDARD.

6 A. I DON'T REMEMBER WHAT IT WAS CALLED AT I.B.M.

7 Q. WERE YOU INVOLVED IN THE DEVELOPMENT OF D.E.S.?

8 A. I WAS INVOLVED INDIRECTLY IN THE DEVELOPMENT, BUT I
9 WAS PRIMARILY INVOLVED IN THE CERTIFICATION PROCESS.

10 Q. AND D.E.S. IS A VERY WIDELY USED SYMMETRIC
11 NON-PUBLIC E CRYPTOGRAPHIC SYSTEM TODAY; IS THAT
12 RIGHT?

13 A. YES.

14 Q. WOULD YOU AGREE WITH ME THAT IN TERMS OF COMMERCE,
15 IT IS PROBABLY THE SINGLE MOST COMMONLY USED SYMMETRIC
16 CRYPTOGRAPHIC SYSTEM?

17 A. WELL, I COULDN'T GIVE YOU FIGURES TO BACK THAT UP,
18 BUT I WOULD NOT FIND THAT SUPRISING AT ALL.

19 Q. AND YOU PLAYED A KEY ROLE IN THE DEVELOPMENT OF
20 THAT, ISN'T THAT RIGHT?

21 A. NO. I SAID THAT I PLAYED A ROLE IN THE
22 DEVELOPMENT, BUT MY PRIMARY ROLE WAS IN THE
23 CERTIFICATION.

24 Q. IS THAT SOMETHING -- WHEN YOU SAY THE PRIMARY ROLE
25 WAS IN THE CERTIFICATION IN PROVING TO THE

1 CRYPTOGRAPHIC COMMUNITY OR RESPONDING TO CRITICISMS OF
2 D.E.S.; IS THAT RIGHT?

3 A. NO. THE RESPONSIBILITY WAS TO THE I.B.M.
4 CORPORATION TO MAKE SURE THAT THIS STANDARD, THIS
5 CRYPTOGRAPHIC ALGORITHM WAS A HIGH QUALITY ALGORITHM
6 AND THAT IT WOULD BE INFEASIBLE TO RECOVER THE KEY IN
7 THE PLAIN TEXT FROM CIPHER TEXT.

8 Q. I WANT TO BE A LITTLE MORE CERTAIN THAT I
9 UNDERSTAND THE DISTINCTION YOU'RE DRAWING FROM BEING
10 INVOLVED IN THE DEVELOPMENT OF D.E.S. TO PURSUING ITS
11 CERTIFICATION. WHAT WAS THE DIFFERENCE?

12 A. THE DIFFERENCE IS THE FOLLOWING. I WAS EMPLOYED
13 BY I.B.M. CORPORATION, BUT I WORKED AT THE THOMAS J.
14 WATSON RESEARCH CENTER WITH MARTY HELLMAN FOR SOME
15 TIME. THE RESEARCH DIVISION NEVER BROUGHT OUT -- AT
16 LEAST IT NEVER BROUGHT OUT UNTIL I LEFT IN 1982 --
17 PROMISE. THESE WERE ASSIGNED TO SPECIFIC DIVISIONS.

18 THE DIVISION IN KINGSTON, NEW YORK WAS
19 CHARTED WITH THE RESPONSIBILITY OF IMPLEMENTING
20 TESTING AND BRINGING OUT D.E.S. AS A PRODUCT FOR
21 I.B.M. OR AT LEAST EMBEDDING IT WITHIN THE SYSTEM. WE
22 HAD A COLLABORATION WITH THAT DIVISION WHICH INVOLVED
23 TALKING TO THE PEOPLE THERE AND HELPING THEM. BUT AT
24 THE SAME TIME, WE BEGAN TO WORK ON OUR OWN IN TRYING
25 TO ASCERTAIN THE STRENGTH OF D.E.S.

1 Q. IT WAS YOUR POSITION, YOUR PERSONAL AND
2 PROFESSIONAL POSITION AT I.B.M. THAT D.E.S. WAS A
3 STRONG CRYPTOGRAPHIC SYSTEM; IS THAT CORRECT?

4 A. THAT'S MY POSITION THEN AND NOW.

5 Q. AND THAT WAS A POSITION THAT YOU ADVOCATED FAIRLY
6 VIGOROUSLY; ISN'T THAT RIGHT?

7 A. I'M NOT SURE IF I ADVOCATED IT VIGOROUSLY, BUT I
8 ADVOCATED IT.

9 Q. WAS YOUR VIEW UNIVERSALLY SHARED IN THE
10 CRYPTOGRAPHIC COMMUNITY?

11 A. I WON'T SAY THAT IT WAS NOT SHARED. MANY PEOPLE
12 IN THE CRYPTOGRAPHIC COMMUNITY HAD QUESTIONS ABOUT
13 D.E.S. MARTY HELLMAN WAS ONE WHICH HAD QUESTIONS
14 WHICH WERE LEGITIMATE QUESTIONS AFFECTING THE STRENGTH
15 OF D.E.S., AND THEY VOICED THOSE QUESTIONS TO THE
16 NATIONAL BUREAU OF STANDARDS, HAD TWO WORKSHOPS THAT
17 WERE DEVOTED TO ISSUES CONNECTED WITH THIS BEFORE THE
18 CERTIFICATION OF D.E.S. WAS COMPLETED.

19 Q. WAS PROFESSOR HELLMAN INVOLVED IN FACT IN MAKING
20 SPECIFIC SUGGESTIONS OF HOW TO CHANGE D.E.S. TO AVOID
21 THE WEAKNESSES HE SAID WERE PRESENT?

22 A. IF I UNDERSTOOD PROFESSOR HELLMAN'S COMMENT,
23 PROFESSOR HELLMAN FELT THAT A KEY AMP OF 56 BITS WAS
24 NOT SUFFICIENT AND, THEREFORE, WOULD ALLOW AS
25 TECHNOLOGY IMPROVED AN OPONENT TO BUILD THE MACHINE

1 THAT COULD TEST ALL OF THE KEYS AND DETERMINE WHAT THE
2 PLAIN TEXT WAS. AND HE ADVOCATED THAT THE NATIONAL
3 BUREAU OF STANDARDS AND I.B.M. BRING OUT A PRODUCT
4 WITH A LONGER KEY.

5 Q. WAS THAT THE ONLY SUGGESTION THAT PROFESSOR
6 HELLMAN HAD?

7 A. NO. I DON'T REMEMBER EXACTLY ALL OF THE
8 QUESTIONS, BUT I THINK THAT HE AND OTHERS FELT THE
9 FOLLOWING. THERE WERE CERTAIN DESIGN PRINCIPLES THAT
10 WERE USED IN THE DESIGN OF D.E.S. SOME OF THESE
11 PRINCIPLES EVOLVED FROM I.B.M. SOME OF THESE
12 PRINCIPLES EVOLVED FROM THE NATIONAL SECURITY AGENCY
13 WHICH REQUESTED THAT I.B.M. NOT DIVULGE THEM OUTSIDE
14 OF THE I.B.M. COMMUNITY. AND I.B.M. AGREED TO DO
15 THIS, AND THESE DESIGN PRINCIPLES WERE NOT MADE
16 PUBLIC.

17 PROFESSOR HELLMAN AND MAYBE OTHERS FELT THAT
18 THERE WAS SOMETHING, A TRAP DOOR IN D.E.S. WHICH WOULD
19 ALLOW PEOPLE, NAMELY THE GOVERNMENT OR PEOPLE WHO KNEW
20 THE TRAP DOOR, TO BREAK THE SYSTEM. SO HE HAD
21 ADVOCATED A FULL DISCLOSURE OF THIS, BUT I.B.M. HAD
22 AGREED, AND I ABIDED BY I.B.M.'S RULES NOT TO DIVULGE
23 THIS INFORMATION. I MIGHT ADD THAT IN 20 YEARS, NO
24 ONE HAS FOUND ANYTHING.

25 Q. SO JUST SO I'M CLEAR, PROFESSOR HELLMAN IN FACT

1 DIDN'T SAY, "OH, YOU SHOULD USE LARGER KEY SIZE." HE
2 AND OTHERS SAID D.E.S. MAY HAVE A FUNDAMENTAL WEAKNESS
3 THAT MAKES IT INSECURE; ISN'T THAT RIGHT?

4 A. WELL, I CAN'T -- I CAN'T ATTEST TO THE WORDS HE
5 SAID. HE SAID 56 WAS NOT LONG ENOUGH.

6 Q. I'M TRYING TO UNDERSTAND THE DIFFERENCE. HE HAD
7 ONE COMMENT ABOUT THE KEY SIZE. BUT I ASKED YOU IF
8 THAT WAS THE ONLY CRITICISM HE HAD, AND YOU SAID THERE
9 WAS ONE AND THAT'S DIFFERENT CRITICISM THAN KEY SIZE.

10 A. IT'S NOT THAT HE ASSERTED THAT THERE WAS A
11 WEAKNESS BUT THAT HE ASSERTED THAT I.B.M. SOME BE MORE
12 FORTHCOMING AND REVEAL THE DESIGN PRINCIPLE.

13 Q. DIDN'T PROFESSOR HELLMAN ALSO ADVOCATE A DIFFERENT
14 CRYPTOGRAPHIC SYSTEM INSTEAD OF D.E.S.?

15 A. I'M NOT FAMILIAR IF HE DID.

16 Q. ISN'T IT TRUE THAT PROFESSOR HELLMAN AND STANFORD
17 UNIVERSITY ARGUED THAT HIS CRYPTOGRAPHIC SYSTEMS WERE
18 MORE SECURE BECAUSE THEY DIDN'T HAVE THE UNEXPLAINED
19 FEATURES DEVELOPED BY THE M.S.A.?

20 A. ARE YOU REFERRING TO THE TRAP DOOR KNAPSACK? IS
21 THAT WHAT YOU MEAN?

22 Q. ANY OTHER SYSTEM OTHER THAN D.E.S.

23 A. I'M NOT SURE IF HE ADVOCATED THAT.

24 Q. ISN'T IT TRUE THAT YOU AND PROFESSOR HELLMAN HAVE
25 BEEN PROFESSIONALLY DISAGREEING ABOUT D.E.S. FOR MORE

1 THAN A DECADE?

2 A. I WOULD NOT SAY THAT AT ALL. IF FACT, WHEN I
3 APPLIED FOR MY POSITION AT U.C.S.B., I WROTE MARTY
4 HELLMAN. AND THIS WAS IN 1982, OVER SIX YEARS AFTER
5 WE'VE HAD THIS DISCUSSION. AND AS FAR AS I KNOW,
6 MARTY HELLMAN WROTE A LETTER. OF COURSE HE MAY HAVE
7 SAID BAD THINGS ABOUT ME, BUT I DON'T THINK HE DID
8 BECAUSE I GOT AN APPOINTMENT AT U.C.S.B.

9 SO IF I WERE AT SUCH ODDS WITH HIM, HE
10 CERTAINLY WOULD HAVE NEVER WRITTEN, AND HE WOULD NEVER
11 HAVE WRITTEN THE WONDERFUL THINGS HE SAID ABOUT ME TO
12 THE UNIVERSITY OF CALIFORNIA; SO I DON'T THINK THAT.
13 MARTY HELLMAN AND I DISAGREE. I DON'T THINK IT WAS A
14 PROBLEM. IF I HAD MY OWN WAY, MAYBE I WOULD CHANGE MY
15 MIND, BUT I DON'T THINK THIS WAS A PERSONAL
16 DISAGREEMENT WHICH MADE US ENEMIES. AT LEAST I HOPE
17 NOT.

18 MR. FLINN: THANK YOU, SIR.

19 THE COURT: MR. SCHLAFLY?

20 CROSS-EXAMINATION

21 BY MR. SCHLAFLY: Q. I HAVE A COUPLE OF
22 QUESTIONS. I BELIEVE YOU TESTIFIED THAT THE ALGORITHM
23 THAT BECAME THE DATA ENCRYPTION STANDARD WAS DEVELOPED
24 AROUND 1970; IS THAT CORRECT?

25 A. I'M NOT SURE, MR. SCHLAFLY, OF THE EXACT DATE. IN

1 '67 AN ALGORITHM CALLED LUCIFER WAS DEVELOPED, AND
2 D.E.S. IS A VARIOUS ON LUCIFER. IT MAY HAVE OCCURRED
3 OVER A PERIOD OF TWO OR THREE YEARS. I DON'T KNOW THE
4 EXACT DATES OF THE DEVELOPMENT.

5 Q. BUT COULD YOU SAY IT WAS WITHIN TWO OR THREE YEARS
6 OF 1970?

7 A. YES, I BELIEVE SO.

8 Q. AND IS IT YOUR OPINION THAT THE D.E.S. WAS SECURE
9 IN 1976?

10 A. YES, IT'S MY OPINION.

11 Q. DO YOU HAVE AN OPINION AS TO WHETHER OR NOT THAT
12 ALGORITHM WAS SECURE IN 1970?

13 A. AS FAR AS I KNOW, THE SAME ALGORITHM WAS -- MUST
14 HAVE BEEN THE SAME ALGORITHM IN 1970. SO I THINK IT
15 WAS SECURE ALSO IN 1970.

16 Q. HAD IT BEEN CERTIFIED IN 1970?

17 A. NO, IT HAD NOT BEEN CERTIFIED WITH THE NATIONAL
18 BUREAU OF STANDARDS IN 1970.

19 Q. SO YOU'RE WILLING TO SAY IN YOUR USE OF THE WORD
20 SECURE THAT THE ALGORITHM THAT BECAME THE DATA
21 ENCRYPTION STANDARD WAS SECURE IN 1970 BUT HAD NOT
22 BEEN CERTIFIED AS SECURE IN 1970?

23 A. IT'S MY OPINION THAT D.E.S. WAS SECURE IN 1970.
24 AT THAT TIME THE PROCESS WITHIN I.B.M. OF CERTIFYING
25 IT WAS IN PROGRESS, AND THE PROCESS DEVELOPED BY THE

1 GOVERNMENT TO CERTIFY D.E.S. AS A NATIONAL STANDARD
2 WAS SET INTO PLAY EITHER IN 1970 OR 1971. AND IT WAS
3 COMPLETED AT A TIME WHICH ALLOWED THE NATIONAL BUREAU
4 OF STANDARDS TO MAKE IT A STANDARD IN 1976.

5 IT HAS ALSO BEEN RECERTIFIED SEVERAL TIMES.
6 I DON'T HAVE THE DATES OF THAT RECERTIFICATION. IT
7 MAY BE EVERY 10 YEARS IT COMES UP FOR
8 RECERTIFICATION. IT HAS BEEN RECERTIFIED TWICE TO THE
9 BEST OF MY KNOWLEDGE ON THAT MATTER.

10 Q. ARE YOU AWARE OF A PATENT ON THE DATA ENCRYPTION
11 STANDARD?

12 A. YES.

13 Q. ARE YOU LISTED AS AN INVENTOR?

14 A. NO, I AM NOT AN INVENTOR OF D.E.S.

15 Q. CAN YOU EXPLAIN WHY YOU'RE NOT LISTED AS AN
16 INVENTOR?

17 A. WELL, BECAUSE I WAS NOT AN INVENTOR.

18 Q. BUT YOU DID HAVE AN ACTIVE ROLE IN CERTIFYING IT.

19 A. I DID HAVE AN ACTIVE ROLE IN CERTIFYING IT, AND I
20 REMEMBER VISITING KINGSTON WITH SOME OF MY COLLEAGUES
21 AND DISCUSSING THE PROCESS OF THE DESIGN OF D.E.S.

22 Q. WOULD YOU SAY IT'S FAIR TO SAY THAT INVENTING A
23 SECURE CRYPTOSYSTEM IS SOMETHING ENTIRELY DIFFERENT
24 FROM CERTIFYING A SECURE CRYPTOSYSTEM?

25 A. IT MOST CERTAINLY IS THE CASE. INVENTING IS

1 DIFFERENT THAN PROVING SECURE OR ATTEMPTING TO CERTIFY
2 A SYSTEM.

3 Q. SUPPOSE I WERE TO TELL YOU THAT I HAVE ON MY LAP
4 TOP OVER HERE A CRYPTOGRAPHIC PROGRAM THAT I WROTE
5 MYSELF AND HAS NEVER BEEN PUBLISHED. WOULD YOU SAY
6 IT'S NECESSARILY INSECURE?

7 A. I DON'T EVEN KNOW WHAT THE ALGORITHMS ARE. I
8 WOULD CERTAINLY NOT VENTURE AN OPINION BEFORE LOOKING
9 AT IT.

10 Q. SO YOU COULDN'T SAY WHETHER IT'S SECURE OR NOT
11 BASED ON THE INFORMATION THAT I TOLD YOU?

12 A. SINCE I HAVE NO IDEA WHAT ALGORITHM YOU HAVE
13 IMPLEMENTED, I WOULD VENTURE NO OPINION AS TO ITS
14 SECURITY.

15 Q. IT MIGHT POSSIBLY BE SECURE AND MIGHT POSSIBLY BE
16 INSECURE?

17 A. QUITE CORRECT.

18 Q. I HAVE TROUBLE RECONCILING THAT WITH YOUR
19 STATEMENTS EARLIER THAT A CRYPTOSYSTEM CANNOT BE
20 SECURE UNLESS ITS BEEN PUBLISHED AND CERTIFIED
21 SECURE. CAN YOU EXPLAIN THAT CONTRADICTION?

22 A. I TOOK AS MY DEFINITION THAT A SECURE SYSTEM TO
23 HIDE INFORMATION IS A SYSTEM WHICH MEETS -- HAS TWO
24 ATTRIBUTES. ONE, THAT THE SYSTEM OFFERS GUARANTEES IN
25 THE FORM OF REPEATED ATTACKS BY PEOPLE WHO ARE

1 COMPETENT TO MAKE THESE ATTACKS AND THAT THIS PROCESS
2 OFFERS THE GUARANTEE OF SECRECY OVER A CERTAIN PERIOD
3 OF TIME. SO THAT'S WHAT A SECURE CRYPTOGRAPHIC SYSTEM
4 IS.

5 NOW, YOU'VE SAID TO ME THAT ON YOUR PC THERE
6 YOU'VE GOT A CRYPTOGRAPHIC SYSTEM. FINE. I'M NOT
7 GOING TO SAY TO YOU THAT IT'S SECURE, INSECURE UNTIL I
8 STUDY IT.

9 Q. OKAY. BUT I ALSO TOLD YOU THAT IT'S UNPUBLISHED
10 AND HAS NOT BEEN SUBJECTED TO THESE CRYPTOGRAPHIC
11 ATTACKS BY EXPERTS IN THE FIELD.

12 A. I'M NOT GOING TO SAY THAT IT IS SECURED.

13 Q. BUT IT MIGHT BE SECURE?

14 A. IT MIGHT BE SECURE, QUITE CORRECT.

15 Q. YOU MIGHT SAY IT MIGHT BE SECURE. YOU WOULD
16 PROBABLY HAVE NO FAITH IN ITS SECURITY, BUT IT MIGHT
17 STILL BE SECURE ANYWAY.

18 A. I'M NOT GOING TO VENTURE A GUESS. I HAVEN'T EVEN
19 LOOKED AT IT. HOW CAN I MAKE A JUDGMENT UPON
20 SOMETHING WHICH I HAVEN'T EVEN LOOKED AT?

21 Q. ARE YOU PREPARED TO SAY THAT YOU HAVE NO FAITH IN
22 ITS SECURITY UNLESS IT HAS BEEN SCRUTINIZED?

23 A. ABSOLUTELY CORRECT. I WOULD NOT SAY THAT THE
24 SYSTEM -- THAT YOU CAN USE THE WORD COMMUNICATING
25 SECURELY UNTIL YOU HAVE TAKEN WHATEVER ALGORITHM

1 YOU'VE PROPOSED AND SUBJECT IT TO SCRUTINY AS THE
2 AUTHORS OF THIS INVENTION HAVE SAID IN THEIR PAPER
3 REPEATEDLY, NOT ONCE BUT THREE TIMES.

4 Q. SO IT WOULD BE FAIR TO SAY THAT CRYPTOSYSTEM MIGHT
5 BE SECURE, BUT YOU HAVE NO FAITH IN ITS SECURITY.

6 A. IT MIGHT BE SECURE, AND I HAVE NO WAY OF KNOWING
7 IF IT'S SECURE. I'M NOT GOING TO TELL YOU WHETHER I
8 HAVE FAITH IN IT OR NOT. YOU'VE ASKED ME A QUESTION.
9 I DON'T CONSIDER IT SECURE UNTIL SOMEBODY HAS LOOKED
10 AT IT, NOT ONLY ONE PERSON BUT SEVERAL PEOPLE AND MADE
11 A PRUDENT INVESTIGATION OF ITS SECURITY.

12 MR. SCHLAFLY: NO FURTHER QUESTIONS.

13 THE COURT: ANY FURTHER WITNESSES?

14 MR. HASLAM: I JUST HAVE TWO QUESTIONS FOR
15 THIS WITNESS.

16 REDIRECT EXAMINATION

17 BY MR. HASLAM: Q. WE'VE GOT CLAIM ONE UP
18 HERE. THIS IS WHAT YOU UNDERSTAND AT LEAST TO
19 CORRESPOND TO ONE OF THE EMBODIMENTS IN THE PATENT?

20 A. YES, MR. HASLAM.

21 Q. IS THERE ANY LANGUAGE IN CLAIM ONE THAT SPEAKS TO
22 THE ISSUE OF AUTHENTICATION?

23 A. THERE IS NOTHING IN CLAIM ONE THAT TALKS ABOUT
24 AUTHENTICATION.

25 Q. AND THE REFERENCE TO AUTHENTICATION IS IN A

1 DIFFERENT CLAIM WHICH MAY SPEAK TO A DIFFERENT
2 EMBODIMENT?

3 A. IT'S IN A DIFFERENT CLAIM.

4 MR. HASLAM: I HAVE NO FURTHER QUESTIONS.

5 MR. KENNEDY: NOTHING FURTHER HERE, YOUR
6 HONOR.

7 MR. FLINN: NOTHING HERE, YOUR HONOR.

8 THE COURT: WE CAN TAKE A 15-MINUTE RECESS
9 AND GO TO 3:15. IS THAT SATISFACTORY?

10 MR. HASLAM: I BELIEVE THAT WE COULD GET THE
11 WITNESS ON AND OFF ON DIRECT. I DON'T KNOW WHAT THE
12 CROSS IS GOING TO BE. I WOULD THINK WE COULD GET DONE
13 WITH 45 MINUTES OR AN HOUR OF GETTING THIS WITNESS ON
14 AND OFF AND COMPLETED. IT DEPENDS ON HOW FAR RANGE WE
15 WANT TO GO AGAIN ON CROSS.

16 THE COURT: LET'S SAY THE 15 MINUTES. IN 15
17 MINUTES WE'LL RESUME.

18 (A RECESS WAS TAKEN.)

19 THE COURT: NEXT WITNESS.

20 MR. HASLAM: I'D LIKE TO CALL STEVEN DUSSE.

21 STEVEN DUSSE

22 CALLED AS A WITNESS ON BEHALF OF THE PLAINTIFF, FIRST
23 BEING DULY SWORN, TESTIFIED AS FOLLOWS:

24 THE WITNESS: I DO.

25 THE CLERK: PLEASE STATE YOUR NAME AND SPELL

1 YOUR LAST FOR THE COURT.

2 THE WITNESS: MY NAME IS STEVE DUSSE,
3 D-U-S-S-E.

4 THE CLERK: WHAT IS YOUR OCCUPATION, SIR?

5 THE WITNESS: MY OCCUPATION IS CHIEF
6 TECHNOLOGY OFFICER.

7 THE COURT: PROCEED.

8 DIRECT EXAMINATION.

9 BY MR. HASLAM: Q. YOU INDICATED YOU'RE A
10 CHIEF TECHNOLOGY OFFICER. FOR WHOM DO YOU WORK?

11 A. RSA DATA SECURITY.

12 Q. WHAT WERE YOU ASKED TO DO PRIOR TO COMING HERE
13 TODAY?

14 A. I WAS ASKED TO READ THE CLAIM NUMBER SIX OF
15 PATENT '582 IN ORDER TO COME TO AN UNDERSTANDING FROM
16 THE CLAIM AND SPECIFICATIONS OF THE PATENT AND HOW TO
17 DESIGN HARDWARE CIRCUITRY TO IMPLEMENT THE INVENTION
18 SPECIFIED.

19 Q. AND AS A RESULT OF YOUR REVIEW OF THE PATENT, DID
20 YOU COME TO A CONCLUSION AS TO WHAT THE CIRCUIT
21 ELEMENTS DESCRIBED OR SHOWN IN THE PATTERN ARE
22 PERFORMING THE FUNCTIONS STATED IN CLAIM SIX?

23 A. YES, I DID.

24 Q. CAN YOU VERY BRIEFLY JUST GIVE US AN OVERVIEW OF
25 YOUR BACKGROUND AND EDUCATION IN SO FAR AS IT RELATES

1 TO CIRCUIT DESIGN OR HARDWARE ELEMENTS.

2 A. YES. FROM 1981 TO 1985, I ATTENDED M.I.T. I
3 RECEIVED A BACHELOR OF SCIENCE DEGREE IN ELECTRICAL
4 ENGINEERING IN A CONCENTRATION IN HARDWARE DESIGN AND
5 TOOK SEVERAL COURSES IN HARDWARE DESIGN AND TRANSISTOR
6 AND SEMICONDUCTOR THEORY AS WELL AS SOME MATHEMATIC
7 COURSES.

8 UPON GRADUATING FROM M.I.T., MY FIRST JOB WAS
9 WITH FORD AEROSPACE CORPORATION IN PALO ALTO. WHILE
10 AT FORD AEROSPACE, I DESIGNED HIGH SPEED DIGITAL
11 COMMUNICATION CIRCUITRY FOR SATELLITE COMMUNICATIONS.
12 I JOINED RSA IN MAY OF 1987. MY RESPONSIBILITIES WERE
13 VARIED BECAUSE AS THE FIRST FULL-TIME ENGINEER AT RSA,
14 HAD A NUMBER OF RESPONSIBILITIES.

15 PERTINENT TO MY HARDWARE DESIGN EXPERIENCE, I
16 DESIGNED A PC CARD AT RSA AROUND 1990 WHICH PERFORMED
17 OPERATIONS FOR ACCELERATING CRYPTOGRAPHIC OPERATIONS
18 IN CONJUNCTION WITH A PC. THIS WAS A CARD THAT I
19 DESIGNED USING DIGITAL CIRCUITRY.

20 Q. COULD YOU LOOK FOR A MOMENT AT EXHIBIT 61 WHICH IS
21 IN THE WHITE BINDERS WHICH I THINK WAS A DEPOSITION
22 EXHIBIT AT YOUR DEPOSITION.

23 A. I HAVE MY COPY OF THAT.

24 Q. IS THAT IN THE BINDER? LET ME ASK YOU, IS THE
25 COPY YOU HAVE THERE THE COPY THAT YOU PRODUCED AT YOUR

1 DEPOSITION?

2 A. YES, IT IS.

3 Q. AND CAN YOU JUST BRIEFLY TELL US WHAT -- THERE'S
4 SOME HANDWRITING OR NOTATIONS ON EXHIBIT 61. CAN YOU
5 TELL ME, DID YOU PUT THOSE THERE?

6 A. YES, I DID.

7 Q. CAN YOU JUST TELL US WHAT IT IS THAT YOU DID --
8 HOW YOU WENT ABOUT PUTTING THOSE NOTATIONS ON THERE?

9 A. DURING THE COURSE OF MY INVESTIGATION IN ORDER TO
10 COME TO AN UNDERSTANDING, I MADE SOME HANDWRITTEN
11 NOTES ON SOME OF THE FUNCTIONS ASSOCIATED WITH SOME OF
12 THE FIGURES. AND ALSO IN SPECIFICATION LANGUAGE, I
13 ANNOTATED FOR MYSELF WHERE PARTICULAR DESCRIPTIONS OF
14 HARDWARE CIRCUITRY BEGAN AND ENDED.

15 Q. AND JUST FROM -- YOU CAN LOOK AT THEM NOW IF YOU
16 NEED TO TO ANSWER THIS QUESTION. BUT BASED ON YOUR
17 REVIEW OF THE EXHIBIT 61 WHICH IS THE '582 PATENT,
18 HAVE YOU IN YOUR EDUCATIONAL WORK EXPERIENCE ACTUALLY
19 WORKED WITH COMPONENTS OR CIRCUIT ELEMENTS SUCH AS
20 THOSE DESCRIBED IN THE '582 PATENT?

21 A. YES, I HAVE.

22 Q. IF I COULD, LET ME ASK YOU TO LOOK AT RSA DATA
23 SECURITY INC.'S AMENDED PROPOSED JURY INSTRUCTIONS ON
24 PLAIN CONSTRUCTION. AND IN PARTICULAR IF YOU COULD
25 LOOK AT THE APPENDIX, I'M GOING TO BE ASKING YOU

1 QUESTIONS ABOUT PROPOSED INSTRUCTIONS A.61 THROUGH
2 A.64.

3 I HAVE AN EXTRA COPY HERE IF THE COURT
4 WOULD --

5 THE COURT: YOU'VE GOT ONE? OKAY. PLEASE
6 SEND IT UP.

7 MR. HASLAM: I PUT A YELLOW MARKER, YOUR
8 HONOR, AT THE BEGINNING OF A.61.

9 MR. HASLAM: Q. IF YOU'LL LOOK AT
10 INSTRUCTION A.61 WHICH RELATES TO THE MEANS FOR
11 PROVIDING RANDUM INFORMATION AS A RECEIVER, YOU'LL SEE
12 A REFERENCE THERE TO A COLUMN IN LINE SITE, COLUMN 6,
13 LINE 1 THROUGH 5. DO YOU SEE THAT?

14 A. YES, SIR.

15 Q. DO YOU HAVE AN OPINION AS TO WHETHER THAT
16 REFERENCE ACCURATELY SETS FORTH WHAT THE PATENT
17 DISCLOSES AS THE MEANS FOR PROVIDING RANDUM
18 INFORMATION AT THE RECEIVER?

19 A. I DO HAVE AN OPINION. MY OPINION IS THAT THE
20 ELEMENTS OUTLINED IN JURY INSTRUCTION A.61 DO
21 ACCURATELY DESCRIBE THE STRUCTURES PROVIDED AS THE
22 MEANS FOR PROVIDING RANDUM INFORMATION AT THE
23 RECEIVER.

24 Q. IN AN EFFORT TO EXPEDITE THIS, HAVE YOU PRIOR TO
25 TODAY REVIEWED PROPOSED INSTRUCTIONS A.62 THROUGH A.64

1 WITH RESPECT TO THE REFERENCES IN EACH OF THOSE
2 INSTRUCTIONS TO THE FIGURES AND REFERENCES TO THE
3 SPECIFICATION? HAVE YOU DONE THAT?

4 A. YES, I HAVE.

5 Q. AND BASED ON THAT, HAVE YOU COME TO AN OPINION OR
6 CONCLUSION AS TO WHETHER THE FIGURES AND CITATIONS IN
7 THOSE INSTRUCTIONS, A.61 THROUGH A.64, ACCURATELY SET
8 FORTH THE MEANS WHICH ARE DISCLOSED FOR CARRYING OUT
9 THE STATED FUNCTIONS IN EACH OF THOSE INSTRUCTIONS?

10 MR. FLINN: OBJECTION, YOUR HONOR. I WANT TO
11 MAKE CLEAR THAT THE OBJECTION IS INSTRUCTED TO THE
12 STRUCTURES OF THE PATENT BECAUSE THIS WITNESS CANNOT
13 TALK ABOUT THE HARDWARE, AND THAT'S WHAT I WANT TO
14 MAKE SURE THE QUESTION GETS AT.

15 MR. HASLAM: THE QUESTION IS WITH REFERENCE
16 TO THE FIGURES AND THE CITATIONS TO THE SPECIFICATION
17 IN THE INSTRUCTIONS ACCURATELY SET FORTH A DESCRIPTION
18 OF THE STRUCTURES DISCLOSED OR THE MEANS DISCLOSED FOR
19 CARRYING OUT THE FUNCTION.

20 THE COURT: OKAY.

21 THE WITNESS: WITH TWO MINOR CORRECTIONS,
22 THAT IS MY OPINION.

23 MR. HASLAM: Q. WHAT CORRECTIONS?

24 A. ON A.62 THERE ARE SOME CITATIONS WHICH I FEEL ARE
25 MISSING, COLUMN 7, LINE 44 THROUGH COLUMN 9, LINE 4

1 SHOULD BE INCLUDED IN THE FIRST PARAGRAPH ON A.62
2 UNDER THE TITLE "PUBLIC ENCIPHERING KEY."

3 Q. WHAT WAS THAT?

4 A. THE ADDITION OF COLUMN 7, LINE 44 THROUGH COLUMN
5 9, LINE 4 AT THE END OF THE FIRST PARAGRAPH UNDER THE
6 HEADING "PUBLIC ENCIPHERING KEY."

7 Q. CAN YOU TELL US WHAT'S BEING DESCRIBED IN THOSE.

8 A. YES. COLUMN 7, LINE 44 THROUGH COLUMN 9, LINE 4
9 DISCLOSES SOME OF THE SPECIFICATIONS FOR THE KEY
10 GENERATOR FOR GENERATING THE PUBLIC ENCIPHERING KEY IN
11 WHAT'S KNOWN AS THE FIRST EMBODIMENT.

12 Q. AND I BELIEVE YOU SAID YOU HAD ONE OTHER
13 CORRECTION THAT YOU THOUGHT WAS NECESSARY?

14 A. THAT'S CORRECT.

15 Q. WHERE IS THAT?

16 A. ON THE NEXT PAGE, AJ 21 UNDER THE HEADING "SECRET
17 DECIPHERING KEY," THE SECOND PARAGRAPH.

18 THE COURT: OKAY. THE SECOND PARAGRAPH
19 STARTING WITH THE "MEANS DISCLOSED"?

20 THE WITNESS: CORRECT.

21 THE COURT: OKAY.

22 THE WITNESS: THAT PARAGRAPH ENDS IN A
23 CITATION FOR COLUMN 12, LINE 33 THROUGH COLUMN 13,
24 LINE 6. I BELIEVE THAT SHOULD GO THROUGH COLUMN 13,
25 LINE 8.

1 MR. HASLAM: Q. AND THAT WOULD BY EXTENDING
2 THOSE TWO LINES WOULD PICK UP THE REFERENCE TO THE
3 BASE B WHICH IS USED IN GENERATING THE SECRET KEY IN
4 THE SECOND EMBODIMENT?

5 A. IN THE SECOND EMBODIMENT, THAT'S CORRECT.

6 Q. LET ME JUST ASK YOU FOR A MOMENT TO GO TO FIGURE
7 11 IN THE PATENT, EXHIBIT 61. DO YOU HAVE THAT IN
8 FRONT OF YOU?

9 A. YES, I DO.

10 THE COURT: WHAT SHEET IS THIS?

11 MR. HASLAM: FIGURE 11. IT'S EITHER IN
12 EXHIBIT 61 OR EXHIBIT 13. THEY ARE BOTH COPIES OF
13 THE '582 PATENT.

14 THE COURT: THE TABLE?

15 MR. HASLAM: YES.

16 Q. CAN YOU TELL US WHAT'S BEING DEPICTED IN FIGURE
17 11?

18 A. WHAT'S BEING DEPICTED IN FIGURE 11 IS A CIRCUIT
19 DIAGRAM FOR A KEY GENERATER WHICH IS DESCRIBED IN THE
20 SPECIFICATION AS THE SECOND EMBODIMENT FOR GENERATING
21 A SECRET DECIPHERING KEY AND A PUBLIC ENCIPHERING KEY.

22 Q. I NOTICE THERE ARE VARIOUS BLOCKS THAT ARE LABELED
23 ON THE TABLE, EXPONENTIATOR, MULTIPLIER, ET CETERA.
24 IS THERE ANYTHING IN THE PATENT WHICH DESCRIBES OR
25 DEPICTS WHAT CIRCUIT ELEMENTS GO IN THOSE BOXES?

1 A. YES. IN A NUMBER OF CASES, THERE ARE DESCRIPTIONS
2 OF EACH BOX AND MORE DISCRETE CIRCUIT ELEMENTS WHICH
3 ARE USED TO CONSTRUCT THOSE. AN EXAMPLE OF THAT IS
4 EXPONENTIATOR UP IN THE UPPER RIGHT CORNER OF THAT
5 FIGURE WHICH IS FURTHER DEFINED BY FIGURE 10 ON THE
6 PRECEDING PAGE TO BE CONSTRUCTED OF THREE REGISTERS
7 AND A MULTIPLIER.

8 Q. IN OTHER WORDS, FIGURE 10 WOULD BE PUT IN THE BOX
9 WHERE THE EXPONENTIATOR IS?

10 A. THAT'S CORRECT, THAT'S MY OPINION.

11 Q. AND I NOTICE IN FIGURE 10, THERE'S A BOX 124 THAT
12 SAYS "MULTIPLIER."

13 A. THAT'S CORRECT. THAT MULTIPLIER IS FURTHER
14 DEFINED IN ANOTHER FIGURE EARLIER, FIGURE 3.

15 Q. FIGURE 3 THEN SHOWS AN EXAMPLE OF THE MULTIPLIER?

16 A. THAT'S CORRECT.

17 Q. SO FIGURE 3 WOULD GO INTO THE BOX LABELED 124 IN
18 FIGURE 10?

19 A. THAT'S CORRECT.

20 Q. I NOTICE ON FIGURE 3 THERE'S A REFERENCE TO AN
21 ADDER, SUBTRACTOR, AND A COMPARITOR -- BOXES 55, 56
22 AND 57. DO YOU SEE THOSE?

23 A. YES.

24 Q. IS THERE ANYTHING IN THE PATENT WHICH DESCRIBES
25 WHAT THE INVENTORS DISCLOSED AS BEING CONTAINED IN

1 THOSE BOXES?

2 A. YES, THERE IS. THE ADDER IS DESCRIBED AS A SERIES
3 OF GATES IN FIGURE 4. THE COMPARATOR IS DESCRIBED IN
4 FIGURE 5, AND SUBTRACTOR IS DESCRIBED IN FIGURE 6, ALL
5 ON THE SAME PAGE.

6 Q. NOW, ARE THE CIRCUIT ELEMENTS WHICH ARE DESCRIBED
7 IN THESE VARIOUS FIGURES YOU POINTED OUT CONFIGURED AS
8 DESCRIBED AND SHOWN IN THE PATENT IN ANY PARTICULAR
9 WAY?

10 A. WELL, THE GATES ARE WIRED IN SUCH A WAY AS TO
11 PERFORM THE FUNCTIONS THAT ARE DESCRIBED. IN OTHER
12 WORDS, THE CONNECTIONS THAT ARE MADE FROM ONE GATE TO
13 ANOTHER ACTUALLY DICTATE THE FUNCTION THAT'S PERFORMED
14 BY THE COLLECTION OF GATES IN THAT PARTICULAR
15 CONFIGURATION.

16 A GOOD WAY TO ILLUSTRATE THIS POINT IS TO
17 LOOK AT BOTH FIGURE 4 AND FIGURE 6. IF YOU NOTICE,
18 THEY HAVE ROUGHLY THE SAME NUMBER AND TYPE OF GATES.
19 HOWEVER, THE ADDITION AND SUBTRACTION FUNCTIONS WHICH
20 THEY PERFORM ARE VERY DIFFERENT BASED LARGELY ON THE
21 DIFFERENT CONNECTIONS THAT ARE MADE BETWEEN THOSE
22 GATES.

23 Q. SO IN OTHER WORDS, YOU CAN TAKE THE SAME ELEMENTS
24 THAT ARE IN FIGURE FOUR AND IN FIGURE SIX AND,
25 DEPENDING ON HOW YOU CAN FIGURE THEM, END UP

1 PERFORMING A DIFFERENT FUNCTION?

2 A. THAT'S CORRECT.

3 Q. GOING BACK TO FIGURE 11 FOR A MOMENT. ARE THE
4 CIRCUIT ELEMENTS IN FIGURE 11 CONFIGURED TO PERFORM
5 ANY SPECIFIC FUNCTION?

6 A. YES, THEY ARE CONFIGURED TO PERFORM KEY GENERATION
7 FUNCTION IN THE SECOND EMBODIMENT WHICH IS DESCRIBED
8 IN TEXTUAL AND MATHEMATIC TERMS IN THE SPECIFICATION
9 OF THE PATENT BEGINNING ON COLUMN 12, LINE 33 AND
10 ENDING ON COLUMN 16, LINE 23.

11 Q. ARE THE CIRCUIT ELEMENTS WHICH ARE DESCRIBED IN
12 FIGURE 11 INTERCHANGEABLE IN THE SENSE THAT, IF I
13 MODIFY THE WAY IN WHICH THEY WERE INTERCONNECTED, THEY
14 WOULD PERFORM THE SAME FUNCTION THAT THEY DO AS
15 DESCRIBED?

16 A. IT'S NOT VERY LIKELY THAT, IF ANY OF THE
17 INTERCONNECTIONS OR ANY OF THE CIRCUIT ELEMENTS WERE
18 INTERCHANGED THAT IT WOULD PERFORM THE SAME
19 MATHEMATICAL FUNCTION. A GOOD EXAMPLE MIGHT BE
20 SWITCHING THE ADDER AND MULTIPLIER IN FIGURE 11.

21 RATHER THAN TAKING A MULTIPLICATIVE
22 CUMULATION OF A BUNCH OF TERMS, IT WOULD TAKE AN
23 ADDATIVE CUMULATION. AND RATHER THAN ADDING BY ONE
24 WHICH INCREMENTS A NUMBER IT WOULD MULTIPLY BY ONE
25 WHICH WOULD COME OUT AS THE SAME NUMBER. SO IT'S VERY

1 UNLIKELY THAT THE SAME RESULT WOULD BE ACHIEVED BY
2 EITHER REARRANGING THE INFORMATION OR INTERCHANGING
3 THE PARTS.

4 Q. ARE THE CIRCUIT ELEMENTS DESCRIBED IN THE '582
5 PATENT AND SHOWN IN THE FIGURES OF THE '582 PATENT
6 SPECIFICALLY CONFIGURED TO PERFORM SPECIFIC
7 MATHEMATICS?

8 A. YES, THEY ARE.

9 Q. WHAT MATHEMATICS IS THAT?

10 A. THOSE ARE THE MATHEMATICS DESCRIBED IN THE
11 SPECIFICATION FOR THE FIRST AND SECOND EMBODIMENT.

12 Q. AND ARE THE CIRCUIT ELEMENTS DESCRIBED AND SHOWN
13 IN THE AMENDED JURY INSTRUCTIONS WE SAW DIRECTED BY
14 YOU SPECIFICALLY CONFIGURED TO PERFORM THE STATED
15 FUNCTION OF CLAIM SIX BY PERFORMING THOSE SPECIFIC
16 MATHEMATICS?

17 A. YES, THEY ARE.

18 MR. HASLAM: I HAVE NO OTHER QUESTIONS.

19 MR. KRAMER: KARL KRAMER ON BEHALF OF
20 CARO-KANN AND CYLINK.

21 CROSS-EXAMINATION

22 BY MR. KRAMER: Q. MR. DUSSE, WE'VE TALKED
23 TOGETHER BEFORE ABOUT THIS CASE AT THE DEPOSITION. DO
24 YOU REMEMBER THAT?

25 A. YES.

1 Q. DO YOU RECALL IN THAT DEPOSITION I ASKED YOU
2 WHETHER YOU HAD IDENTIFIED IN YOUR ANALYSIS THE
3 STRUCTURES IN THE PATENT?

4 A. NO, I DON'T RECALL.

5 Q. DO YOU RECALL IN YOUR DEPOSITION EXPLAINING TO ME
6 THE STRUCTURES IN THE PATENT THAT ALIGNED WITH THE
7 VARIOUS MEANS ELEMENTS OF CLAIM SIX?

8 A. YES, I DO.

9 Q. IN YOUR TESTIMONY TODAY, I'M A LITTLE UNCLEAR AS
10 TO WHAT THE EFFECT OF YOUR TESTIMONY IS INTENDED TO
11 BE. ARE YOU ADOPTING WORD-FOR-WORD THE DESCRIPTION IN
12 EACH OF JURY INSTRUCTIONS A.62 THROUGH A.64?

13 A. NO. IT'S MY OPINION THAT THOSE JURY INSTRUCTIONS
14 ACCURATELY REFLECT THE SPECIFICATIONS AND FIGURES FOR
15 THE PARTICULAR CLAIMS THAT ARE LISTED AT THE TOP OF
16 THE JURY INSTRUCTIONS FOR THE PERFORMING -- FOR
17 PERFORMING THE INVENTION THAT'S DESCRIBED.

18 Q. FOR EXAMPLE, IS IT YOUR TESTIMONY THAT THE
19 STRUCTURES INVOLVE THE KNAPSACK EMBODIMENT THAT'S
20 DISCLOSED IN THE PATENT? IS THAT YOUR TESTIMONY
21 TODAY?

22 A. IT IS.

23 MR. KRAMER: YOUR HONOR, I'M GOING TO
24 APPROACH THE WITNESS AND PRESENT HIM WITH SEVERAL
25 DOCUMENTS, THE FIRST OF WHICH IS HIS TRANSCRIPT.

1 Q. MR. DUSSE, CAN YOU SHOW ME WHERE IN THERE IN
2 RESPONSE TO ANY QUESTION I ASKED ABOUT IDENTIFICATION
3 OF STRUCTURES IN THE PATENT DID YOU USE THE WORD
4 "KNAPSACK"?

5 A. I DON'T RECALL USING THE WORD KNAPSACK IN MY
6 DEPOSITION.

7 Q. DO YOU RECALL IN THERE TESTIFYING THAT THE
8 STRUCTURES WERE LIMITED IN ANY WAY BY ANY MATHEMATICAL
9 OPERATION?

10 A. I DON'T UNDERSTAND YOUR QUESTION.

11 Q. WHAT DON'T YOU UNDERSTAND ABOUT THE QUESTION?

12 A. CAN YOU REPEAT THE QUESTION, PLEASE.

13 Q. WELL, I GUESS WE'LL HAVE TO GO AT IT ONE MEANS AT
14 A TIME HERE. YOU'LL NOTE THE SECOND MEANS IDENTIFIED,
15 THE MEANS FOR GENERATING FOR RANDUM INFORMATION A
16 PUBLIC ENCIPHERING KEY. DO YOU SEE THAT?

17 A. YES.

18 Q. COULD YOU TURN TO PAGES 53 AND 54 OF YOUR
19 TESTIMONY, PLEASE.

20 THE COURT: WHERE IS IT LOCATED? WHAT
21 NUMBER?

22 MR. KRAMER: THAT WOULD BE PAGES 53 AND 54.

23 THE COURT: OKAY.

24 MR. KRAMER: BEGINNING ON PAGE 53, LINE 15.

25 THE COURT: 15. OKAY. QUESTION.

1 MR. KRAMER: Q. DO YOU RECALL THIS LINE,
2 THE QUESTIONING WHERE WE WERE --

3 THE COURT: "COULD YOU TELL ME BY COLUMN AND
4 LINE AND NUMBER THE HARDWARE ELEMENTS THAT YOU BELIEVE
5 ARE THE STRUCTURES FOR ELEMENT 1,B?"

6 THE WITNESS: YES, I DO RECALL.

7 MR. KRAMER: Q. YOU IDENTIFIED FOR ME THE
8 MULTIPLIER, CORRECT, WHICH IS IN FIGURE 3.

9 A. YES.

10 Q. DID YOU SAY ANYTHING IN THAT TESTIMONY ABOUT THE
11 KNAPSACK?

12 A. NO, SIR.

13 Q. NOW, I UNDERSTAND THAT THE NEXT MEANS ELEMENT, THE
14 MEANS FOR COMMUNICATING THE PUBLIC ENCIPHERING KEY,
15 YOU DID NOT ADDRESS AT ALL, CORRECT, IN YOUR TESTIMONY
16 AT THE DEPOSITION, MEANS FOR COMMUNICATING THE PUBLIC
17 ENCIPHERING KEY?

18 A. THAT'S CORRECT. I DID NOT ADDRESS THAT IN MY
19 DEPOSITION.

20 Q. LET'S MOVE ON TO MEANS FOR ENCIPHERING A MESSAGE
21 AT THE TRANSMITTER. DO YOU SEE THAT UP THERE?

22 A. YES.

23 Q. LET'S TURN TO PAGE 61 OF YOUR TESTIMONY. I
24 BELIEVE WE CALLED THAT ELEMENT 1,D WHEN WE WERE
25 DISCUSSING THE CLAIM; IS THAT CORRECT?

1 A. YES.

2 Q. I ASKED YOU AT LINE 10 "WHAT ARE THE STRUCTURAL
3 ELEMENTS OF THE PATENT THAT CORRESPONDS TO THE ELEMENT
4 1,D?" DO YOU SEE THAT?

5 A. YES.

6 Q. COULD YOU READ YOUR RESPONSE FOR ME.

7 A. "STRUCTURAL ELEMENTS ARE DEFINED IN FIGURE 2."

8 Q. AND THEN I ASKED YOU "IS THAT THE ONLY PLACE THEY
9 ARE?" WHAT DID YOU SAY IN YOUR RESPONSE?

10 A. I SAID, "YES."

11 Q. NOW, IF WE MOVE ON TO THE NEXT MEANS ELEMENT,
12 MEANS FOR TRANSMITTING THE ENCIPHERED MESSAGE, YOU
13 DIDN'T TESTIFY ABOUT THAT ELEMENT AS WELL, DID YOU.

14 A. THAT'S CORRECT.

15 Q. FINALLY, LET'S MOVE ON TO THE FINAL ELEMENT AND
16 MEANS FOR DECIPHERING SET ENCIPHERED MESSAGE AT THE
17 RECEIVER. IN YOUR DEPOSITION AT PAGE 63, YOU
18 TESTIFIED ABOUT THAT ELEMENT, DIDN'T YOU.

19 A. YES.

20 Q. AND I ASKED YOU AT LINE THREE, "WHAT STRUCTURAL
21 ELEMENTS IN THE '582 HELLMAN-MERKLE PATENT CORRESPONDS
22 TO ELEMENT 1?" DO YOU SEE THAT?

23 A. YES.

24 Q. YOU FIRST POINTED TO FIGURE 7; CORRECT?

25 A. THAT'S CORRECT.

1 Q. AND THEN AT LINE 11 OF PAGE 64, I ASKED YOU "IS
2 THERE ANY OTHER STRUCTURE ELEMENT THAT YOU BELIEVE
3 CORRESPONDS TO ELEMENT ONE?" DO YOU SEE THAT?

4 A. YES.

5 Q. AND YOU IDENTIFIED FIGURE 9; CORRECT?

6 A. THAT'S CORRECT.

7 Q. SO FOR NONE OF THE ELEMENTS THAT YOU COVERED IN
8 YOUR DEPOSITION DID YOU REFER TO THE KNAPSACK; ISN'T
9 THAT CORRECT?

10 A. NOT BY TERM, NO.

11 Q. MR. DUSSE, HOW LONG HAVE YOU BEEN INVOLVED IN
12 CRYPTOGRAPHY?

13 A. I'VE BEEN INVOLVED IN CRYPTOGRAPHY SINCE JOINING
14 IN THE EMPLOYMENT OF RSA DATA SECURITY IN MAY OF 1987.

15 Q. SO NINE YEARS?

16 A. NINE-AND-A-HALF YEARS.

17 Q. WHILE YOU WERE AT RSA, YOU HAVE WORKED ON A
18 PROJECT CALLED BSAFE; IS THAT CORRECT?

19 A. THAT'S CORRECT.

20 Q. IN FRONT OF YOU I THINK IS A MANUAL ENTITLED
21 "BSAFE USERS MANUAL VERSION 2.1." COULD YOU LOOK AT
22 THAT FOR A SECOND, PLEASE. NOW, IS THIS A DOCUMENT
23 THAT YOU ARE FAMILIAR WITH?

24 A. I AM FAMILIAR WITH IT.

25 Q. DID YOU PARTICIPATE IN THE CREATION OF THIS

1 DOCUMENT?

2 A. I PARTICIPATED IN THE REVIEW OF THIS DOCUMENT BUT
3 NOT THE CREATION.

4 Q. AND DID YOU PARTICIPATE IN THE REVIEW IN THE SENSE
5 THAT YOU REVIEWED IT FOR ACCURACY?

6 A. THAT'S CORRECT.

7 Q. LET'S LOOK TO PART TWO OF THIS DOCUMENT ENTITLED
8 CRYPTOGRAPHY -- AND I BELIEVE IT BEGINS ON PAGE 37.
9 IF YOU LOOK AT THE TABLE OF CONTENTS -- WHY DON'T WE
10 JUST LOOK AT THE TABLE OF CONTENTS HERE WHICH IS
11 PAGE THREE OF THE DOCUMENT UNDER THE HEADING
12 "CRYPTOGRAPHY TERMONOLOGY." IS THAT A SECTION WHERE
13 YOU INTRODUCE THE READER TO BASIC TERMS USED IN MODERN
14 CRYPTOGRAPHY?

15 A. YES, IT SEEMS TO BE.

16 Q. WHILE AT RSA DID YOU BECOME FAMILIAR WITH A
17 DOCUMENT ENTITLED "FREQUENTLY ASKED QUESTIONS ABOUT
18 TODAY'S CRYPTOGRAPHY"?

19 A. ONLY VERY PERIPHERALLY.

20 Q. EXHIBIT 512 -- WOULD YOU TURN TO IT PLEASE
21 AND TELL ME WHETHER YOU'RE FAMILIAR WITH THIS
22 DOCUMENT.

23 A. I'M FAMILIAR WITH ITS EXISTING.

24 THE COURT: WHERE IS THIS?

25 MR. KRAMER: ANOTHER DOCUMENT, EXHIBIT 512.

1 IT SHOULD BE IN THE STACK THAT WAS HANDED UP TO YOU.

2 MR. HASLAM: I REALIZE AT THIS TIME HE'S
3 ASKING TO LOOK AT IT. I'LL OBJECT AS BEING BEYOND THE
4 SCOPE OF DIRECT EXAMINATION, AND IT'S RATHER CLEAR, I
5 BELIEVE, IN LAW THAT YOU CONSTRUE THE CLAIMS WITHOUT
6 RESORTING TO WHAT IS THE ACCUSED PRODUCT WHICH IS WHAT
7 THIS MANUAL BSAFE DEALS WITH.

8 I MEAN, IF THE ARGUMENT IS WE GO TO THE
9 INTRINSIC AND EXTRINSIC EVIDENCE, I'M NOT SURE WHAT
10 THE DEFENDANTS WOULD CALL THIS EVIDENCE THAT WE'RE
11 GOING INTO NOW. I'LL OBJECT TO THAT ON GROUNDS ON
12 RELEVANCE.

13 MR. KRAMER: THE RELEVANCE WILL BECOME
14 APPARENT QUICKLY. IT GOES TO THE USAGE OF
15 TERMINOLOGY.

16 THE COURT: OVERRULED. "FREQUENTLY ASKED
17 QUESTIONS"?

18 MR. KRAMER: Q. PLEASE TURN TO PAGE 39.
19 THERE'S AN ACKNOWLEDGMENT FOR YOUR PROVISION OF
20 INFORMATION AND HELPFUL SUGGESTIONS. DO YOU SEE THAT,
21 PAGE 39 OF FREQUENTLY ASKED QUESTIONS?

22 A. YES.

23 Q. IS THAT ACCURATE? DID YOU PROVIDE INFORMATION AND
24 HELP WITH SUGGESTIONS FOR THIS DOCUMENT?

25 A. YES.

1 Q. AND YOU'VE CERTAINLY REVIEWED IT BEFORE; CORRECT?

2 A. NO.

3 Q. YOU'VE NEVER SEEN THIS DOCUMENT BEFORE?

4 A. I HAVE SEEN IT BEFORE BUT HAVE NEVER REVIEWED IT,
5 NO.

6 Q. IS IT A DOCUMENT THAT'S PRODUCED BY RSA?

7 A. IT'S PRODUCED BY RSA LABS.

8 Q. WHY IS IT PRODUCED?

9 A. I SUPPOSE IT'S MEANT TO BE INFORMATIVE.

10 Q. ON THE COVER IT SAYS IT'S AN "INTRODUCTION TO
11 MODERN CRYPTOGRAPHY." DO YOU SEE THAT, THE FIRST
12 SENTENCE ON THE FIRST PAGE?

13 A. YES, I DO.

14 Q. ON PAGE NINE IT IDENTIFIES SOMEONE NAMED
15 MR. BIDZOS, PARAGRAPH NINE, PAGE 39. WHO IS HE?

16 A. THE MAN WHO SIGNS MY PAYCHECK. HE'S THE PRESIDENT
17 AND CEO OF RSA DAVIS.

18 Q. AND ALSO AT PAGE SEVEN OF THIS DOCUMENT, CAN YOU
19 LOOK AT THE DESCRIPTION OF WHAT IS RSA. IT IDENTIFIES
20 THREE GENTLEMEN -- RON RIVET, ADIR SHAMIR, AND LEONARD
21 ADDLEMAN. DO YOU SEE THAT?

22 A. YES.

23 Q. ARE THE R, S, AND A OF RSA?

24 A. YES.

25 Q. ARE THEY FOUNDERS OF RSA?

1 A. THEY ARE THE INVENTORS OF THE RSA PUBLIC E
2 CRYPTOSYSTEM.

3 Q. WOULD YOU TURN TO EXHIBIT 23 IN THE BINDER SET IN
4 FRONT OF YOU. THERE'S A BINDER IN THE BOX THERE THAT
5 HAS EXHIBIT 23 IN IT.

6 THE COURT: WHAT'S THE EXHIBIT NUMBER?

7 MR. KRAMER: EXHIBIT 23.

8 THE COURT: NOTES ON THE VALIDITY OF THE
9 STANDARD.

10 MR. KRAMER: Q. IS THIS A DOCUMENT PREPARED
11 BY RON RIVET?

12 A. IT PURPORTS TO BE.

13 Q. WOULD YOU TURN TO EXHIBIT 24, PLEASE. THIS IS A
14 MEMO DATED NOVEMBER 13, 1991 FROM JIM BIDZOS. DO YOU
15 SEE THAT?

16 A. YES, I DO.

17 Q. IS THAT THE MR. BIDZOS WHO IS YOUR BOSS?

18 MR. HASLAM: OBJECTION, LACKS FOUNDATION IF
19 HE'S TRYING TO ESTABLISH A FOUNDATION TO THE WITNESS
20 BY THIS QUESTION.

21 THE COURT: EXHIBIT NO. 24?

22 MR. KRAMER: YES.

23 THE COURT: ARE YOU OPPOSING THE USE OF THIS
24 EXHIBIT?

25 MR. HASLAM: I'M OBJECTING TO THAT QUESTION

1 AS LACKING IN FOUNDATION. HE HASN'T ESTABLISHED A
2 FOUNDATION THAT THE WITNESS KNOWS THIS DOCUMENT WAS
3 PREPARED BY MR. BIDZOS.

4 THE COURT: DO YOU HAVE ANY QUESTIONS THAT
5 WILL HELP?

6 MR. KRAMER: Q. WERE YOU TOLD BY ANYONE AT
7 RSA THAT YOUR BOSS HAD PREPARED A MEMO IN WHICH YOUR
8 BOSS CONCLUDED AT THE THIRD TO THE LAST PARAGRAPH OF
9 THE DOCUMENT, "THESE QUESTIONS ARE IMPORTANT BECAUSE
10 CLAIM ONE HAS A VERY BROAD DESCRIPTION THAT APPLY TO
11 ANY PUBLIC E CRYPTOSYSTEM"?

12 A. I WAS NOT TOLD THAT, NO.

13 Q. LET'S TURN BACK TO EXHIBIT 23 WHICH, I BELIEVE, IS
14 THE "FREQUENTLY ASKED QUESTIONS." I GUESS WE'LL CALL
15 IT EXHIBIT 512, PAGE SIX OF THAT DOCUMENT.

16 THE COURT: WHICH DOCUMENT?

17 MR. KRAMER: THIS IS 512, "FREQUENTLY ASKED
18 QUESTIONS ABOUT TODAY'S CRYPTOGRAPHY."

19 THE COURT: ALL RIGHT. WHAT PAGE?

20 MR. KRAMER: PARAGRAPH 1.5 ON PAGE SIX.

21 Q. DO YOU SEE THE SENTENCE BEGINNING "THE BASIC IDEAS
22 OF PUBLIC KEY CRYPTOGRAPHY ARE CONTAINED IN U.S.
23 PATENT," AND THEN IT MENTIONS THE DIFFIE-HELLMAN
24 PATENT, AND THE HELLMAN-MERKLE PATENT. DO YOU SEE
25 THAT?

1 A. YES.

2 Q. DID YOU REVIEW THAT AT ALL IN COMING TO YOUR
3 CONCLUSION THAT THE STRUCTURES ARE SOMEHOW LIMITED TO
4 THE KNAPSACK?

5 A. NO.

6 Q. DO YOU UNDERSTAND WHAT DIGITAL SIGNALS ARE?

7 A. EXCUSE ME?

8 Q. DO YOU UNDERSTAND WHAT DIGITAL SIGNALS ARE?

9 A. IN SPECIFIC CONTEXT, YES.

10 Q. WHAT SPECIFIC CONTEXT DO YOU UNDERSTAND DIGITAL
11 SIGNALS IN?

12 A. IN THE CONTEXT OF MUSIC, DIGITAL SIGNALS ARE
13 SIGNALS OF SOUND THAT HAVE BEEN DIGITIZED SO THEY CAN
14 MANIPULATE DIGITALLY.

15 Q. DO YOU UNDERSTAND THAT TO HAVE ANYTHING TO DO WITH
16 THE CASE?

17 A. NO.

18 Q. IN THE CONTEXT OF CRYPTOGRAPHY IN THE WORK THAT
19 YOU DO, WHAT DOES DIGITAL SIGNALS MEAN?

20 A. I DON'T THINK THERE IS ENOUGH CONTEXT TO COME UP
21 WITH AN ACCURATE DESCRIPTION.

22 Q. WHAT IS -- YOU DON'T KNOW WHAT A DIGITAL SIGNAL
23 IS?

24 A. IN SPECIFIC CONTEXT, YES.

25 Q. WELL, I TRIED TO GIVE YOU A CONTEXT WHICH IS THE

1 WORK THAT YOU DO.

2 A. THAT'S NOT SPECIFIC ENOUGH. DIGITAL SIGNALS CAN
3 APPLY TO MANY DIFFERENT --

4 THE COURT: HAVE YOU USED THAT TERM IN ANY
5 WORK YOU DO SPECIFICALLY, ANY WORK WITH DIGITAL
6 SIGNALS?

7 THE WITNESS: NO.

8 MR. KRAMER: Q. WASN'T YOUR UNDERGRADUATE
9 DEGREE IN DIGITAL HARDWARE DESIGN?

10 A. YES, IT WAS.

11 Q. WHAT DID THE WORD DIGITAL MEAN IN GETTING YOUR
12 DEGREE IN HARDWARE DESIGN?

13 A. DIGITAL REFERRED TO THE BINARY NATURE OF THE
14 REPRESENTATION OF THE SIGNALS -- ONE'S AND ZERO'S.

15 Q. DO YOU KNOW WHAT SIGNALS MEANS IN THE CONTEXT OF
16 HARDWARE? DOES IT MEAN ELECTRICAL IMPULSE?

17 A. IN SOME CONTEXT, YES, IT MEANS ELECTRICAL IMPULSE.

18 Q. IN WHAT CONTEXT WOULD IT NOT BE?

19 A. THERE HAVE BEEN SIGNALING SCHEMES WHICH USE LIGHT.

20 Q. DO YOU UNDERSTAND THAT THOSE SORTS OF SIGNALING
21 MEANS HAVE ANYTHING TO DO WITH THE CASE, THIS CASE?

22 A. NO.

23 Q. SO IN MOST CIRCUMSTANCES RELATING TO YOUR WORK,
24 DIGITAL SIGNALS MEANS ONE'S AND ZERO'S SENT AS
25 IMPULSES, ELECTRICAL IMPULSES; ISN'T THAT CORRECT?

1 A. IN THE CONTEXT OF HARDWARE DESIGN, THAT'S CORRECT.

2 Q. DO YOU KNOW WHAT A PROCESSOR IS?

3 A. I KNOW WHAT SEVERAL DEFINITIONS FOR PROCESSOR,
4 YES.

5 Q. IN THE CONTEXT OF CRYPTOGRAPHY, WHAT IS A
6 PROCESSOR?

7 A. I DON'T THINK THAT THERE'S A SPECIFIC ENOUGH
8 CONTEXT FOR THE DEFINING OF PROCESSOR.

9 Q. IN THE '582 PATENT, THE DISCLOSURE THAT YOU LOOKED
10 AT IN THIS CASE, WHAT IS A DIGITAL PROCESSOR?

11 A. I DON'T THINK THAT THAT'S SPECIFIC ENOUGH CONTEXT
12 EITHER BECAUSE I BELIEVE THAT THERE HAVE BEEN
13 DIFFERENT USES OF THE TERM PROCESSOR FOR DIFFERENT
14 TRANSFORMATIONS OR PROCESSES.

15 Q. HAVE YOU EVER HEARD THE PHRASE CPU?

16 A. YES, I HAVE.

17 Q. WHAT DOES THE P IN CPU STAND FOR?

18 A. PROCESSING.

19 Q. HAVE YOU EVER HEARD THE PHRASE SPECIAL PURPOSE
20 PROCESSOR?

21 A. NO.

22 Q. YOU'VE NEVER HEARD OF SPECIAL PURPOSE PROCESSOR?

23 A. NO.

24 Q. DO YOU AGREE THAT IN THE CONTEXT OF A DIGITAL
25 SIGNAL PROCESSOR, PROCESSING IS THE ACT OF

1 TRANSFORMING DIGITAL SIGNALS FOR MANIPULATING DIGITAL
2 SIGNALS?

3 A. YES, I DO.

4 Q. DO YOU BELIEVE WHAT'S DISCLOSED IN THE PATENT, THE
5 '582 PATENT THAT YOU REVIEWED IS NOT A DIGITAL SIGNAL
6 PROCESSOR?

7 A. THAT'S CORRECT.

8 Q. WHY IS IT NOT A DIGITAL SIGNAL PROCESSOR?

9 A. A DIGITAL SIGNAL PROCESSOR IS A TERM WELL-KNOWN IN
10 THE ART OF HARDWARE DESIGN TO MEAN A CHIP WHICH TAKES
11 AS INPUT DIGITAL SIGNAL PROCESSES AND UNDER A FIRM
12 LAYER OF SOFTWARE CONTROL MANIPULATES OR TRANSFORMS
13 THESE SIGNALS.

14 Q. WHAT ABOUT THE HARDWARE DISCLOSED IN THE PATENT
15 THAT IS NOT A PROCESSOR?

16 A. I'M SORRY. I DON'T UNDERSTAND THE QUESTION.

17 Q. DO YOU UNDERSTAND WHAT'S DISCLOSED IN THE PATENT
18 PROCESSES DATA?

19 A. YES, I DO.

20 Q. IS THAT DATA DIGITAL DATA?

21 A. YES, I BELIEVE IT IS.

22 Q. AND IS THE DIGITAL DATA SENT AS SIGNALS?

23 A. I SUPPOSE THEY ARE.

24 Q. WHEN YOU WERE GIVEN THE TASK OF PREPARING FOR YOUR
25 TESTIMONY IN THIS CASE, YOU DID READ THE CLAIMS,

1 DIDN'T YOU?

2 A. YES, I DID.

3 Q. AND WHEN YOU FIRST READ THOSE CLAIMS, YOU
4 UNDERSTOOD THEM, DIDN'T YOU?

5 A. NO, I DID NOT.

6 Q. WOULD YOU TURN TO YOUR TESTIMONY AT PAGE 36, LINE
7 7 THROUGH 13 OF YOUR TRANSCRIPT.

8 THE COURT: WHAT PAGE?

9 MR. KRAMER: PAGE 36, 7 THROUGH 13, LINES 7
10 THROUGH 13.

11 THE COURT: OKAY. THE QUESTION ASKED INTO
12 CLARIFICATION, THAT PART?

13 MR. KRAMER: YES.

14 Q. "DID YOU ASK FOR ANY CLARIFICATION OF MR. HASLAM'S
15 OPINION OF THE TERMS IN THE CLAIMS?" WHAT DID YOU
16 ANSWER?

17 A. "NO."

18 Q. "NO." I ASKED YOU IS THAT BECAUSE YOU READ THEM
19 AND UNDERSTOOD THEM. WHAT DID YOU SAY?

20 A. I SAID "YES."

21 Q. HAVE YOU HEARD THE WORD GENERATING USED IN THE
22 SENSE OF GENERATING A KEY BEFORE?

23 A. I HAVE HEARD IT USED, YES.

24 Q. DID YOU NOT UNDERSTAND WHAT PEOPLE MEANT WHEN THEY
25 SAID GENERATING THE KEY?

1 A. TYPICALLY, THAT PHRASE IS USED WITHIN THE CONTEXT
2 OF A SPECIFIC ALGORITHM. IN THIS SENSE, YES, I DO
3 UNDERSTAND WHAT THEY MEAN.

4 Q. WOULD YOU TURN TO EXHIBIT 512, "FREQUENTLY ASKED
5 QUESTIONS." THIS IS A DOCUMENT CREATED AND
6 DISSEMINATED BY RSA, IS IT NOT?

7 A. YES, IT IS.

8 Q. LET'S TURN TO PAGE 16, PARAGRAPH 3.3 BEGINS "HOW
9 DOES ONE GET A KEY PAIR?" DO YOU SEE THAT?

10 A. YES.

11 Q. AND THE NEXT, "EACH USER SHOULD GENERATE HIS OR
12 HER OWN KEY PAIR." DO YOU SEE THAT?

13 A. YES, I DO.

14 Q. DO YOU SEE THE WORD GENERATED IN THE NEXT
15 PARAGRAPH? DO YOU SEE THAT?

16 A. YES, I DO.

17 Q. IS THERE ANY DESCRIPTION AT ALL ABOUT A PARTICULAR
18 ALGORITHM?

19 A. NO, THERE IS NOT.

20 Q. YOU BELIEVE THAT RSA WOULD USE SUCH TERMS PEOPLE
21 WOULD NOT UNDERSTAND IN THEIR LITERATURE?

22 A. I DON'T FEEL COMFORTABLE TO GIVE AN OPINION ON
23 WHAT --

24 Q. WHAT THE WORDS MEAN?

25 A. WHAT OUR COMPANY BELIEVES AS A WHOLE.

1 Q. LET'S LOOK AT BSAFE 2.1, WHICH IS MARKED AS
2 EXHIBIT 511. LET'S TURN TO PAGE 56 OF THAT DOCUMENT.

3 THE COURT: WHAT PAGE?

4 MR. KRAMER: PAGE 56.

5 Q. WHAT'S THE TITLE AT THE TOP OF THAT PAGE?

6 A. "KEY GENERATION."

7 Q. CAN YOU READ THAT PARAGRAPH FOR ME.

8 A. "TECHNIQUES FOR GENERATING PUBLIC PRIVATE KEY
9 PAIRS AND SYMMETRIC KEYS ARE QUITE DIFFERENT.
10 SYMMETRIC KEY ALGORITHMS GENERALLY REQUIRE AN
11 ARBITRARY RANDOM BYTE SEQUENCE WHILE A PUBLIC PRIVATE
12 KEY PAIR MUST SATISFY A MATHEMATICAL FORMULA.

13 KEY GENERATION DEPENDS ON THE AVAILABILITY OF
14 A GOOD RANDOM NUMBER GENERATOR AND THE SECURITY OF A
15 RANDOM NUMBER GENERATOR DEPENDS ON THE SEED. SEE THE
16 SECTION ON SEED GENERATION, PSEUDO AND RANDOM NUMBER
17 AND SEED GENERATION FOR THE DISCUSSIONS OF THAT."

18 Q. DO YOU SEE WHERE IT SAYS "KEY MANAGEMENT"?

19 A. YES.

20 Q. THE FIRST THING LISTED IT SAYS "GENERATING KEYS".

21 A. YES.

22 Q. DO YOU THINK PEOPLE -- HAVE YOU EVER HEARD OF
23 ANYBODY READING THAT SECTION OF RSA'S BSAFE USER'S
24 MANUAL AND SAYING "OH, MY GOSH, I DON'T KNOW WHAT THAT
25 MEANS"?

1 A. NO, I HAVE NOT HEARD.

2 Q. LET'S LOOK AT THAT WHICH IS THE FREQUENTLY ASKED
3 QUESTIONS, 512 AT PAGE 10, PARAGRAPH 2.7.

4 THE COURT: PAGE AGAIN, PLEASE.

5 MR. KRAMER: PAGE 10, PARAGRAPH 2.7.

6 Q. SEE THE BOTTOM OF THE PAGE, RSA IS SAYING THAT YOU
7 MUST KEEP CERTAIN SIZE KEYS, AND THEN IT SAYS AT THE
8 VERY LAST SENTENCE, "ALTHOUGH THE SECURITY OF AN
9 INDIVIDUAL KEY IS STILL STRONG, WITH SOME FACTORY
10 METHODS, THERE IS ANOTHER SMALL CHANCE THAT THE
11 ATTACKER MIGHT GET LUCKY AND FACTOR IT QUICKLY"?

12 A. YES, I SEE THAT.

13 Q. DO YOU UNDERSTAND THAT TO BE A GUARANTEE OR A
14 WARANTEE THAT THE RSA CRYPTOSYSTEM IS SECURE?

15 A. NO.

16 Q. DO YOU KNOW OF ANYONE AT RSA WHO HAS EVER WARANTED
17 THAT THE RSA CRYPTOSYSTEM WILL NEVER BE BROKEN?

18 A. NO.

19 Q. LET'S TURN TO PAGE 26, PARAGRAPH 4.7 OF
20 "FREQUENTLY ASKED QUESTIONS." DO YOU AGREE THAT
21 ALTHOUGH FACTORING IS STRONGLY BELIEVED TO BE A
22 DIFFICULT MATHEMATICAL PROBLEM, IT HAS NOT BEEN PROVED
23 SO?

24 A. I DON'T HAVE ANY OPINION.

25 Q. SO IT THEREFORE REMAINS A POSSIBILITY THAT ANY

1 FACTOR OR ALGORITHM WILL BE DISCOVERED. DO YOU AGREE
2 WITH THAT?

3 A. I DON'T HAVE AN OPINION. IT'S NOT AN AREA WHICH
4 I'VE BEEN ASKED TO STUDY.

5 Q. HAVE YOU EVER HEARD THE TERM COMPUTATIONALLY
6 INFEASIBLE BE USED BY RSA?

7 A. YES, I HAVE.

8 Q. HAVE YOU EVER HEARD IT USED IN THE CONTEXT OF RSA
9 GUARANTEEING THAT ITS SYSTEM IS SECURE?

10 A. NO.

11 Q. THAT'S BECAUSE THEY GIVE NO SUCH GUARANTEE;
12 CORRECT?

13 A. I DON'T HAVE AN OPINION.

14 MR. KRAMER: I HAVE NO FURTHER QUESTIONS.

15 MR. FLINN: I HAVE NO QUESTIONS, YOUR HONOR.

16 MR. SCHLAFLY: I JUST HAVE A FEW QUESTIONS.

17 I TAKE IT YOU'RE GOING TO WANT TO ADJOURN SHORTLY.

18 THE COURT: YES, ABOUT 10 MINUTES.

19 CROSS-EXAMINATION

20 BY MR. SCHLAFLY: Q. IN CLAIM 6, WHICH IS
21 ON THE SIGN HERE, DO YOU SEE THE SECOND MEANS CLAUSE?

22 A. YES, I DO. IT MEANS FOR GENERATING FOR SET RANDUM
23 INFORMATION, THAT ONE?

24 Q. YES.

25 A. YES, I DO.

1 Q. IS THERE -- IS THERE A DISCLOSURE IN THE
2 HELLMAN-MERKLE PATENT FOR THAT MEANS CLAUSE?

3 A. YES, THERE IS.

4 Q. AND IS THERE DISCLOSED A SECRET DECIPHERING KEY
5 THAT IS DIRECTLY RELATED TO AND COMPUTATIONALLY
6 INFEASIBLE TO GENERATE FROM THE PUBLIC DECIPHERING
7 KEY?

8 A. THERE IS DISCLOSED A MEANS FOR GENERATING THE
9 SECRET DECIPHERING KEY.

10 Q. AND IS IT DIRECTLY RELATED TO AND COMPUTATIONALLY
11 INFEASIBLE TO GENERATE FROM THE PUBLIC DECIPHERING
12 KEY?

13 A. THOSE SEEM TO ME TO BE ATTRIBUTES OF A SECRET
14 DECIPHERING KEY. WHAT I WAS ASKED TO DO WAS FORM AN
15 OPINION AS TO WHETHER THE MEANS FOR GENERATING THAT
16 KEY WERE DISCLOSED. I FEEL I'VE COME TO AN
17 UNDERSTANDING OF HOW THOSE MEANS ARE DESCRIBED, BUT I
18 HAVE NO OPINION AS TO WHETHER OR NOT THOSE ATTRIBUTES
19 ARE APPLICABLE GIVEN THE MEANS.

20 Q. SO YOU DON'T KNOW WHETHER OR NOT THERE ARE MEANS
21 DISCLOSED IN THE SPECIFICATION HAVING ALL THE
22 NECESSARY ATTRIBUTES?

23 A. THERE ARE MEANS DISCLOSED IN THE SPECIFICATION FOR
24 GENERATING THE SECRET DECIPHERING KEY. I HAVE NO
25 OPINION WHETHER OR NOT THOSE ATTRIBUTES HAVE BEEN MET.

1 Q. DO YOU HAVE OPINION AS TO WHETHER OR NOT THIS
2 CLAIM, HELLMAN-MERKLE CLAIM SIX IS LIMITED TO THE
3 DISCLOSED HARDWARE?

4 A. NO, I DON'T.

5 Q. DO YOU HAVE AN OPINION WHETHER SOFTWARE WOULD BE
6 INTERCHANGEABLE WITH THE DISCLOSED HARDWARE THAT YOU
7 DESCRIBED?

8 MR. HASLAM: OBJECT TO THE QUESTION AS BEYOND
9 THE SCOPE OF THIS HEARING.

10 THE COURT: SUSTAINED.

11 MR. SCHLAFLY: THAT'S ALL I HAVE.

12 MR. HASLAM: YOUR HONOR, I JUST HAVE A FEW.

13 THE COURT: YES.

14 REDIRECT EXAMINATION

15 BY MR. HASLAM: Q. MR. KRAMER ASKED YOU A
16 SERIES OF QUESTIONS OR POINTED OUT A SERIES OF
17 QUESTIONS HE ASKED YOU ABOUT HARDWARE OR STRUCTURAL
18 ELEMENTS. DO YOU RECALL MR. KRAMER EVER ASKING YOU
19 HOW THOSE WERE CONFIGURED OR WHAT FUNCTIONS THOSE WERE
20 INTENDED TO PERFORM?

21 A. I'M SORRY. I DON'T UNDERSTAND.

22 Q. IF YOU LOOK AT PAGE 53, I BELIEVE, IS ONE OF THE
23 QUESTIONS THAT MR. KRAMER POINTED YOU TO.

24 A. YES.

25 Q. HE ASKED YOU -- THE QUESTION WAS "TELL HIM WHERE

1 THE HARDWARE ELEMENTS WERE PERFORMED."

2 A. YES.

3 Q. DID MR. KRAMER EVER ASK YOU WHAT FUNCTIONS OR
4 OPERATIONS THOSE HARDWARE ELEMENTS PERFORMED?

5 A. NO.

6 Q. DO YOU RECALL HIM DOING THAT ELSEWHERE?

7 A. IF YOU MEAN THE SPECIFIC FUNCTIONS WITHIN EACH OF
8 THE BOXES, NO, I DON'T RECALL HIM DOING THAT.

9 Q. NOW, YOU ANSWERED SOME QUESTIONS ABOUT SOME TERMS
10 IN CONNECTION WITH EXHIBIT 511, WHICH IS BSAFE.

11 THAT'S A MANUAL ABOUT RSA PRODUCT, ISN'T IT?

12 A. THAT'S CORRECT.

13 Q. IT'S YOUR UNDERSTANDING THAT CUSTOMERS WOULD
14 UNDERSTAND THOSE QUESTIONS TO BE IN THE CONTEXT OF THE
15 RSA PRODUCT?

16 A. THAT'S CORRECT.

17 MR. KRAMER: OBJECTION, THAT CALLS FOR
18 SPECULATION ALSO IS AMBIGUOUS BECAUSE THE REFERENCES
19 IN THE BEGINNING ARE OBVIOUSLY NOT DIRECTED TO BE WITH
20 EMPLOYMENT IN GENERAL.

21 THE COURT: I'LL OVERRULE THE OBJECTION.

22 MR. HASLAM: Q. MR. KRAMER ALSO IN EXHIBIT
23 512 POINTED YOU TO PAGE 16, 3.3, "HOW DOES ONE GET A
24 KEY PAIR." DO YOU RECALL THAT? DO YOU HAVE THAT IN
25 FRONT OF YOU?

1 A. YES, I DO.

2 Q. IF YOU LOOK AT THE PAGE BEFORE AT THE VERY BOTTOM
3 OF THE PAGE, IT SAYS "ALTHOUGH MOST OF THESE KEY
4 MANAGEMENT ISSUES ARISE IN ANY PUBLIC KEY
5 CRYPTOSYSTEM. FOR CONVENIENCE, THEY ARE DISCUSSED
6 HERE IN THE CONTEXT OF RSA." DO YOU HAVE A BELIEF AS
7 TO WHETHER SOMEONE READING THAT WOULD UNDERSTAND THAT
8 THE FOLLOWING DISCUSSION WAS IN THE CONTEXT OF THE RSA
9 SYSTEM?

10 A. IF THEY HAD READ THAT STATEMENT IN ORDER, YES, I
11 DO.

12 Q. DOES THE WORD SIGNALS APPEAR ANYWHERE IN CLAIM
13 SIX?

14 A. NOT THAT I CAN SEE, NO.

15 Q. DOES THE WORD DIGITAL SIGNALS APPEAR ANYWHERE IN
16 CLAIM SIX?

17 A. NO, NOT THAT I CAN SEE.

18 Q. DOES DIGITAL SIGNAL PROCESSOR APPEAR ANYWHERE IN
19 CLAIM SIX?

20 A. NO, NOT THAT I CAN SEE.

21 Q. DOES THE DISCLOSURE OF THE '582 REFERRING TO A CPU
22 OR CENTRAL PROCESSING UNIT?

23 A. NOT TO MY KNOWLEDGE.

24 Q. IS THE MEANS IN THE '582 FOR CARRYING OUT THE
25 STATED FUNCTIONS IN CLAIM SIX SPECIFIC DISCRETE

1 ELEMENTS COMPRISED TO PERFORM THESE FUNCTIONS?

2 A. THE SPECIFICATION AND FIGURES DEFINED DISCRETE
3 ELEMENTS TO PERFORM THOSE FUNCTIONS.

4 MR. HASLAM: I HAVE NO FURTHER QUESTIONS.

5 THE COURT: ANYTHING ELSE.

6 MR. KRAMER: I HAVE ONE FOLLOW-UP QUESTION.

7 RECROSS EXAMINATION.

8 BY MR. KRAMER: Q. YOU TESTIFIED EARLIER
9 THAT YOU ASSISTED IN THE DEVELOPMENT OF HARDWARE FOR
10 CYLINK; CORRECT?

11 A. NO.

12 Q. DID YOU DEVELOP A PC ADD-ON BOARD; IS THAT
13 CORRECT?

14 A. THAT'S CORRECT.

15 Q. IS THAT PC ADD-ON BOARD CALLED A PROCESSOR?

16 A. NO.

17 Q. WHAT DOES P AND C STAND FOR?

18 A. EXCUSE ME?

19 Q. WHAT DOES P AND C STAND FOR?

20 A. PERSONAL COMPUTER.

21 Q. DO YOU UNDERSTAND THAT THE PERSONAL COMPUTER IS A
22 PROCESSOR?

23 A. THE PERSONAL COMPUTER CONTAINS A CENTRAL
24 PROCESSING UNIT, ONE OF THE ELEMENTS YOU REFERRED TO
25 EARLIER.

1 Q. BUT YOU DON'T THINK THE SPECIAL PIECE OF HARDWARE
2 YOU DEVELOPED SHOULD BE CALLED A PROCESSOR?

3 A. IT CONTAINED A PROCESSOR. THAT WOULD BE VERY
4 CONFUSING IF BOTH THE BOARD AND ONE OF THE ELEMENTS ON
5 THE BOARD WERE BOTH CALLED PROCESSORS.

6 Q. BUT IT CONTAINS THEM?

7 A. IT CONTAINS A DIGITAL SIGNAL PROCESSOR.

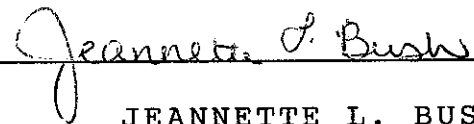
8 MR. KRAMER: THANK YOU.

9 THE COURT: THAT CONCLUDES THE TESTIMONY FOR
10 TODAY. WE'LL RECONVENE AT THIS TIME, AND IT'S
11 SUGGESTED THAT WE MEET AT 9:30 TOMORROW MORNING SO WE
12 GET THE EQUIPMENT OUT AND THEN PROCEED.

13 (COURT SESSION ENDED FOR THE DAY AT 3:12 P.M.)
14
15
16
17
18
19
20
21
22
23
24
25

REPORTER'S CERTIFICATE

I, THE UNDERSIGNED COURT REPORTER FOR THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, DO HEREBY CERTIFY THAT THE FOREGOING IS A FULL, TRUE AND CORRECT TRANSCRIPT OF PROCEEDINGS HAD IN THE WITHIN-ENTITLED AND NUMBERED CAUSE ON THE DATE HEREINBEFORE SET FORTH; AND I DO FURTHER CERTIFY THAT THE FOREGOING TRANSCRIPT HAS BEEN PREPARED BY ME.


JEANNETTE L. BUSH